FORTRA™

Utilizar la Transferencia Segura de Archivos para proteger los datos en la nube

¿Está considerando pasar de operaciones on-premise a una plataforma externa en la nube?

Tal vez solo esté incursionando en el funcionamiento de esta infraestructura. Tal vez haya comenzado a mover partes de su Negocio a la nube y es hora de evaluar las medidas de Seguridad que mejor se adaptan a su nuevo entorno. O tal vez tenga interés en implementar su Negocio en un entorno híbrido.

Cualquiera que sea la etapa en la que se encuentre, una cosa es cierta: no está solo.

Muchas empresas de todo el mundo están desplazando sus sistemas a la informática en la nube con el fin de minimizar su dependencia de la infraestructura de IT interna y de los procesos de negocio complicados. Sin embargo, el estado actual de la Seguridad en la nube es una preocupación real. El 91 % de las organizaciones están preocupadas por la Seguridad en la nube, según el Informe de seguridad en la nube de Cybersecurity Insiders de 2018. Cuando se les preguntó acerca de las mayores barreras que frenan el traslado a la nube, el 39% de los encuestados mencionó riesgos generales de Seguridad.

Lo que plantea la pregunta: ¿está seguro de que sus datos están protegidos? **¿Está su organización en riesgo en la nube?**

¿Qué pasaría si le dijéramos que hay una manera de mejorar la Seguridad de sus datos en la nube, tanto en tránsito como en reposo, para que no tenga que preocuparse por almacenar información confidencial de la empresa fuera de las instalaciones?

Este documento examina el pulso de la nube, desde por qué las empresas están abandonando las operaciones locales hasta el estado actual de la Seguridad en la nube y las transferencias de archivos. Utilice esta guía para explorar cómo una solución sólida de transferencia segura de archivos puede ayudar a proteger las transferencias de datos, en tránsito y en reposo, sin comprometer la conveniencia o la rentabilidad de trasladar su empresa a un entorno basado en la nube.

Prácticas actuales de adopción de la nube

En una encuesta de perspectiva tecnológica de la empresa de contabilidad BDO, el 74 % de los directores financieros que se relacionan con la tecnología dijeron que la informática en la nube tendría el impacto más apreciable en su Negocio en 2017. Además, casi la mitad de las organizaciones prevén que los presupuestos de Seguridad en la nube aumenten en los próximos 12 meses, según el Informe de seguridad en la nube de Cybersecurity Insiders de 2018.
A pesar de este alto porcentaje de inversión, pocas empresas esperan trasladar el 100 % de sus procesos de Negocio a la nube. Gartner, analista del sector, prevé que "el 90% de las organizaciones adoptarán capacidades de administración de infraestructura híbrida" y que "el uso más común de la nube será híbrido" en los próximos tres años.

Transferencia de archivos en la nube

La mayoría de las organizaciones supervisan docenas (si no cientos o miles) de transferencias internas de archivos al día. Ya sea que envíe archivos a los empleados, transfiera informes a socios de Negocio, reciba datos de proveedores externos o recopile información confidencial de clientes, todo es parte del intercambio de información que se procesa regularmente.

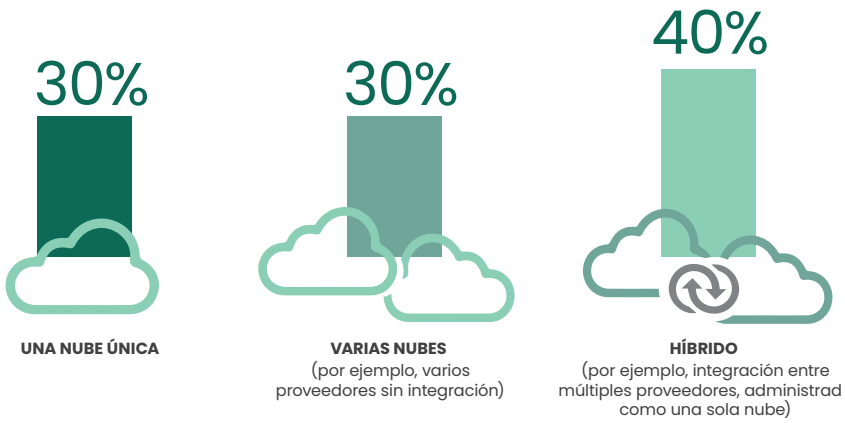
¿Qué sucede con las transferencias de archivos basadas en la nube?

La infraestructura de la nube puede dar a las empresas mucha libertad de acción. Algunos datos se pueden administrar en la nube, o bien, se pueden administrar todos; la elección depende totalmente del usuario. Mover datos a la nube es tan simple como transferir archivos y carpetas a cualquier plataforma de almacenamiento que tenga con su proveedor. Con las políticas de Seguridad y encriptación adecuadas, puede controlar quién tiene acceso a esos datos en la nube.

Los datos que se han confiado a la nube se mantienen en servidores físicos y centros de datos administrados por servicios de informática en la nube. Casi todo el movimiento de archivos entre una empresa, los empleados, los socios de Negocio y las ubicaciones remotas puede realizarse a través de la nube.

La información confidencial puede trasladarse de manera rápida y eficiente entre la empresa y donde sea que esté almacenada (a menudo en servidores de todo el mundo), lo que proporciona a las organizaciones la capacidad de operar sin problemas y acceder a sus datos desde cualquier lugar. Debido a que todo se almacena fuera del sitio, se minimizan las interrupciones locales y los errores de los usuarios, lo que mejora las posibilidades de que las transferencias programadas importantes se completen correctamente.

¿Cuál es su principal estrategia de implementación de la nube?



Fuente: Informe de seguridad en la nube de Cybersecurity Insiders de 2018

Seguridad en la nube

Los beneficios de la nube han hecho que muchas organizaciones adopten, o al menos consideren, algún tipo de entorno de nube. Gartner pronostica que las organizaciones implementadas en la nube experimentarán menos incidentes de Seguridad en los próximos años; en general, los datos almacenados en la nube a menudo se consideran más seguros que los datos guardados en los servidores administrados por una empresa.

Sin embargo, lamentablemente, la pérdida de datos puede afectar, y, de hecho, afecta a quienes se trasladan a un entorno de nube. Tomemos como ejemplo la violación de datos de la RNC de 2017. La empresa de datos que utilizaron colocó una base de datos sin cifrar que contenía la información de 198 millones de votantes estadounidenses en un servidor AWS igualmente desprotegido. Si la empresa hubiera monitoreado rutinariamente la nube en busca de vulnerabilidades, la filtración podría haberse evitado. Pero no fue así.

La realidad es que la nube no es 100 % segura. Debido a eventos como la filtración de datos de RNC, las empresas no están seguras de ceder sus datos a servidores de nube públicos, híbridos y privados. De hecho, la mayoría de los equipos de Ciberseguridad identifican la pérdida de datos, las amenazas a la privacidad de los datos y el incumplimiento de la confidencialidad como sus tres principales preocupaciones de Seguridad en la nube, seguidas del cumplimiento normativo y la soberanía de los datos.

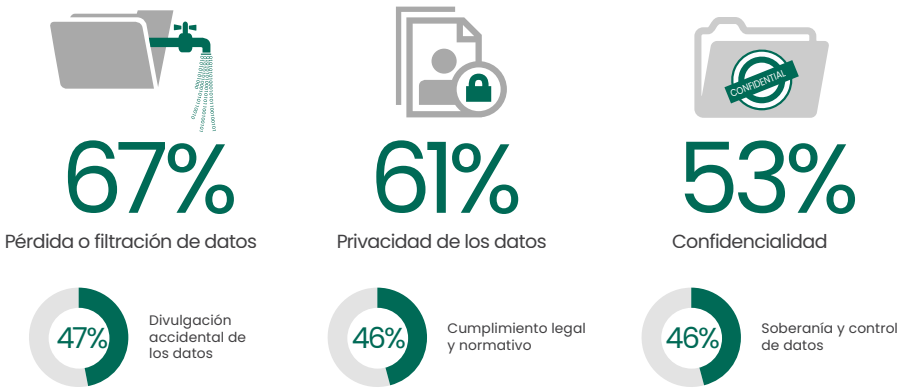
Además, Forbes informa que más del 40 % de las empresas encuestadas han retrasado la implementación de la nube debido a la falta de formación en Ciberseguridad de sus equipos, y solo el 23 % confía plenamente en las plataformas de nube pública para mantener los datos protegidos.

El estado actual de la Seguridad de los datos en la nube

Para las plataformas de informática en la nube como Amazon Web Services, Microsoft Azure y Google Cloud, la Seguridad de los datos de los clientes es una de las prioridades principales. Disponen de una variedad de recursos para proteger la privacidad de sus clientes, pero a pesar de sus mejores intenciones, estas medidas no siempre evitan la pérdida de datos, la información comprometida o las interrupciones inesperadas del servidor en la nube.

La Seguridad en la nube es una responsabilidad compartida. Es imperativo investigar los métodos de Ciberseguridad de cada proveedor de la nube y seleccionar el mejor para su organización: un paso adelante para garantizar la integridad de los datos. Pero este no es el único paso. Los equipos de IT son tan responsables de la Seguridad de sus datos comerciales confidenciales como las plataformas en la nube que los almacenan.

¿Qué es lo que más le preocupa de la Seguridad en la nube?



Fuente: Informe de seguridad en la nube de Cybersecurity Insiders de 2018

Tanto si su organización está pensando en trasladarse a la nube como si ya lo ha hecho, debe realizar la diligencia requerida para los procesos y políticas. Comience por hacerse preguntas como estas:

- ¿Cuáles son las principales consideraciones de Seguridad?
- ¿De qué manera cambiarán nuestros procesos de IT?
- ¿Qué vulnerabilidades han aparecido o cuáles se han solucionado al pasar a la nube?
- ¿Tenemos puntos débiles a los que debemos prestar atención?
- ¿Las transferencias de archivos en la nube están encriptadas correctamente para minimizar el riesgo de filtraciones de datos?

Protección de las transferencias de archivos

Muchas de estas preguntas son subjetivas, por supuesto. Es muy probable que las respuestas varíen según el equipo de IT y las políticas y procesos de su empresa. Para lograr la máxima Seguridad, no omita el estado de las transferencias de archivos.

El cifrado suele ser la última línea de defensa entre un usuario malicioso y la información confidencial. Si los datos están debidamente protegidos durante las transferencias de archivos y cuando se encuentran en un servidor, es menos probable que se produzca una filtración en la nube que termine en la exposición de dichos datos.

Para aquellos que deben cumplir con regulaciones como HIPAA y GDPR, seguir los requisitos de encriptación en la nube tiene beneficios adicionales: siempre que las claves para los datos encriptados sean seguras, la información filtrada no se puede leer, evitando así que los hackers vendan datos confidenciales o de lo contrario, los exploten.

Transferencias de archivos y la nube

Al mover los datos entre la red y la nube, se considera una práctica recomendada cifrar siempre los archivos y proteger la comunicación mediante protocolos de red seguros como SFTP, FTPS o SCP. Los archivos, bases de datos e incluso carpetas enteras también deben encriptarse en reposo, independientemente de si la plataforma en la nube que ha elegido ya los protege.

Un enfoque común para las transferencias de archivos consiste en usar scripts personalizados creados por programadores internos. Los scripts a menudo incluyen comandos para la encriptación, que resultarán más o menos fáciles de modificar en función del conjunto de sus habilidades.

El proceso de transferencia y protección de archivos funcionará durante un tiempo. Aborda inicialmente las necesidades básicas de la empresa. Pero a medida que aumenta la cantidad de transferencias de archivos, también lo hace la dificultad de mantener una solución local, y eso sin tener en cuenta otros posibles obstáculos, como la incapacidad de manejar las capacidades de registro o las alertas cuando se produce un error en una transferencia de archivos.

Las soluciones de transferencia segura de archivos (MFT) proporcionan a las organizaciones funciones útiles que les permiten crecer con sus requisitos de intercambio de datos, lo que es especialmente beneficioso cuando se traslada a un entorno de nube.

GoAnywhere Managed File Transfer

GoAnywhere MFT elimina la necesidad de scripts internos y múltiples programas al agilizar el proceso de transferencia de archivos. Se puede instalar en un entorno basado en la nube u on-premise a través de una variedad de plataformas, lo que le proporciona un control total de la implementación.

Las transferencias se pueden programar y automatizar con flujos de trabajo personalizados (proyectos), y los datos se pueden enviar entre sistemas, empleados, clientes y socios de Negocio. Mientras tanto, los administradores reciben un único punto de control con extensas configuraciones de Seguridad, registros de auditoría e informes, lo que reduce en gran medida la posibilidad de errores y descuidos de los usuarios.

GoAnywhere también proporciona un alto retorno de la inversión al reducir el tiempo dedicado al trabajo manual, mejorar la calidad de las transferencias de archivos, hacer que la Seguridad sea más rentable y ayudar a las organizaciones a cumplir una variedad de requisitos, incluidos PCI DSS, HIPAA, GDPR y FISMA.

Seguridad y encriptación de MFT

En la solución de transferencia segura de archivos de GoAnywhere, todas las transferencias de archivos están protegidas con protocolos de encriptación conocidos, como SFTP, FTPS, AS2 o HTTPS. Un administrador de claves incorporado permite a los administradores crear, importar, exportar y administrar claves Open PGP, claves SSH y certificados SSL.

Para aquellos que deben cumplir con el estándar FIPS 140-2, pueden habilitarse códigos de encriptación validados para los protocolos SSL y SSH. GoAnywhere ofrece conexiones a una variedad de servidores y garantiza la entrega de archivos mediante reintentos de conexión y reanudación automática de archivos. Los administradores pueden comprobar que la transferencia se haga correctamente, revisar la actividad de la cuenta y autenticar el acceso de los usuarios desde cualquier lugar a través de la interfaz basada en navegador de GoAnywhere.

Más allá de las prácticas y características básicas de encriptación, GoAnywhere también aborda varios requisitos comerciales para la nube.

Requisito de la nube	Funcionalidad correspondiente de GoAnywhere
Alertas de actividad Su organización debe saber el momento exacto en que se agrega, elimina o modifica un archivo en la nube.	**Monitoreo de archivos** La función de monitoreo de archivos de GoAnywhere permite a los equipos de IT supervisar carpetas en sistemas basados en la nube y recibir una alerta por correo electrónico cada vez que se activa un evento.
Implementación en plataformas de informática en la nube Su organización desea interactuar con una aplicación externa, como el portal basado en la nube de un socio de Negocio, para enviar y recuperar archivos comerciales importantes, programar transferencias de archivos automatizadas y ejecutar flujos de trabajo avanzados.	**Comandos, API y protocolos de servicios web** GoAnywhere proporciona comandos y API para la integración con aplicaciones externas: líneas de comando del sistema, scripts, lenguajes de programación, programadores de terceros, etc. También se admiten protocolos de servicios web como SOAP y REST, lo que permite una interfaz sencilla con las plataformas informáticas en la nube AWS y Microsoft Azure.
Conexión con socios de Negocio Su organización necesita conectar con socios de Negocio internos y externos en la nube, mientras protege la integridad de las transferencias de archivos posteriores.	**Sistemas de archivos basados en la nube** Los socios de Negocio internos y externos pueden conectarse a su organización a través de carpetas en sistemas de archivos basados en la nube como Amazon S3. GoAnywhere también protege las transferencias entrantes en la nube de las partes interesadas clave con SFTP, FTPS, HTTPS y protocolos AS2.
Procesamiento automático de archivos Su organización quiere que los archivos en la nube se trasladen y se procesen automáticamente, en lugar de manualmente, para ahorrar tiempo y costos de mano de obra.	**Flujos de trabajo programados** Las transferencias de archivos y los flujos de trabajo se configuran fácilmente para mover y procesar archivos en sus entornos de nube y redes privadas. Puede programarlos para que se ejecuten en cualquier momento utilizando el programador integrado de GoAnywhere.
Integración con aplicaciones en la nube Su organización necesita una manera fácil y segura de transferir datos hacia y desde aplicaciones y servicios basados en la web y la nube.	Los Cloud Connectors de GoAnywhere le brindan una integración lista para usar con aplicaciones y servicios web y en la nube conocidos, como Salesforce, JIRA, SharePoint, Microsoft Dynamics CRM, Box y Dropbox, así como un diseñador de conectores en la nube fácil de usar donde puede construir sus propias integraciones.

GoAnywhere y Amazon EC2

Para las organizaciones que utilizan AWS como su proveedor de nube, GoAnywhere MFT se integra fácilmente con Amazon Elastic Cloud Computing (EC2). Puede encontrar e instalar rápidamente GoAnywhere MFT en el AWS Marketplace de Amazon.

Puede utilizar la tecnología FTP segura de GoAnywhere para proteger las transferencias de archivos confidenciales con una tecnología de encriptación sólida y métodos de autenticación modernos. Se crean túneles encriptados entre los sistemas del cliente y del servidor y se proporciona confidencialidad e integridad a las transmisiones críticas. La tecnología FTP segura también protege cualquier credencial de usuario que pase a través de la conexión.

¿Quiere gestionar un gran volumen de transferencias de archivos en su organización? Con la tecnología de agrupación en clústeres de GoAnywhere, las transferencias de archivos y otros procesos se pueden distribuir en varias instancias de Amazon EC2 para equilibrar la carga. Y cuando una instancia se desconecte, las transferencias de archivos y los trabajos se enrutarán automáticamente a otras instalaciones en el clúster.

GoAnywhere y Microsoft Azure

Para las organizaciones que utilizan Microsoft como proveedor de la nube, GoAnywhere se integra con Azure para proporcionar a los equipos de IT transferencias de archivos seguras entre todas las partes activas.

Instalar y ejecutar GoAnywhere MFT en Azure es un proceso sencillo, ya que todo lo necesario está incluido, reduciendo la necesidad de soluciones adicionales de terceros. Puede instalar GoAnywhere en los sistemas operativos Windows o Linux compatibles con Azure que desee, y luego configurar las cuentas de sus socios de Negocio y los procesos de transferencia de archivos.

El diseño intuitivo y las funciones modulares de GoAnywhere le permiten configurar Azure rápidamente.

Si desea escalar GoAnywhere en Azure, las transferencias de archivos y otros procesos se pueden distribuir en varias instancias de Azure VM para equilibrar la carga. Las conexiones a una variedad de bases de datos, como Microsoft SQL Server a través de GoAnywhere, y las cuentas de usuario se pueden autenticar en Microsoft Active Directory para simplificar la administración de usuarios para sus necesidades de colaboración de archivos.

Conclusion

En todo el mundo, las organizaciones se están trasladando a la nube. De hecho, muchas han hecho parcialmente la transición y se sienten optimistas acerca de su futuro. Pero la Seguridad sigue siendo un problema, y migrar a la nube no está exento de riesgos. Para evitar la pérdida de datos, los equipos de IT deben actuar con la diligencia requerida y tomar medidas para proteger sus datos, comenzando con las transferencias de archivos en la nube.

La implementación de una solución de transferencia segura de archivos como GoAnywhere MFT permite a las empresas controlar la protección de sus datos, en tránsito y en reposo. A través de protocolos de encriptación sólidos, monitoreo de archivos e integración con Amazon EC2 y Microsoft Azure, los equipos de IT pueden estar seguros de que sus datos están protegidos en una variedad de entornos sin ejecutar scripts y programas costosos que consumen mucho tiempo.

¿Está a punto para mejorar la Seguridad de sus datos en la nube?

Obtenga la versión de prueba gratuita de 30 días de GoAnywhere MFT.

Solicite una prueba gratuita

FORTRA™

Sobre Fortra

Fortra es una empresa de Ciberseguridad como ninguna otra. Creamos un futuro más simple y sólido para nuestros clientes. Nuestro equipo de expertos junto con el mejor portfolio de soluciones integradas y escalables aportan equilibrio y control a organizaciones en todo el mundo. Somos impulsores del cambio positivo y su aliado de confianza para darle tranquilidad en cada paso de su camino de Ciberseguridad. Conozca más en fortra.com

fta-ga-wp-0523-r1-vm