Marzo de 2021

INFORME DE MERCADO

El estado de las copias de seguridad de Office 365

El paso global al teletrabajo intensifica los retos de la protección de datos. »

Barracuda
Your journey, secured.

Contenido

Introducción

Protección de la explosión de los datos de Office 365

Existe una explosión de los datos de Microsoft Office 365 y una necesidad acuciante de protegerlos.

Office 365 está experimentando un crecimiento tremendo, en particular en el mundo actual de las plantillas remotas. Según Thexyz blog, en marzo de 2020, el número de minutos de reuniones en Teams aumentó en un 380 % en solo los primeros 19 días de la pandemia y ascendió de 560 millones a 2700 millones por día.

Usuarios activos mensuales de O365 (millones)

La ganancia media en usuarios mensuales de Office 365 casi se cuadruplicó desde octubre de 2019 hasta abril de 2020, en gran parte a causa de una mayor confianza en el trabajo colaborativo durante la pandemia.

Los responsables de TI entienden la confianza de sus organizaciones en Office 365 y la necesidad de protección. No obstante, a menudo se da cierta confusión sobre qué características de protección se incluyen o no en la funcionalidad nativa de Office 365.

De hecho, Microsoft recomienda a los clientes que usen copias de seguridad de terceros, ya que la empresa solo garantiza la disponibilidad de su servicio, no la retención de sus datos. Como Microsoft no incluye retención nativa, los clientes podrían no ser conscientes de las limitaciones hasta que se dé un problema.

Los clientes también pueden concluir que las herramientas integradas de Microsoft son básicas y que la restauración con herramientas nativas puede resultar difícil y llevar mucho tiempo. Las organizaciones que buscan proteger sus datos de rápido crecimiento expresan su preocupación por la integridad de las soluciones de copias de seguridad y retención, así como por la seguridad, el cumplimiento normativo y, lo que es más importante, la facilidad de instalación y uso de esa solución.

Este informe aborda las preocupaciones y las preferencias de los profesionales de la TI respecto a Office 365, la seguridad de los datos, las copias de seguridad y la recuperación, las soluciones de software como servicio (SaaS) y temas relacionados.

Metodología

Barracuda le encargó a la consultora de investigación de mercado independiente Centropy que pusiera en marcha una encuesta con los responsables de las tomas de decisiones de TI al respecto de la infraestructura de nube de sus organizaciones. Participaron en ella **1828 responsables de toma de decisiones de TI** de empresas con 50 o más empleados en los **EE. UU., EMEA y APAC**. La encuesta se llevó a cabo en enero de 2021.

Hallazgos clave

HALLAZGO N.º 1

La protección de los datos frente a ataques y pérdidas—tanto de agentes externos como de fuentes internas—es una cuestión fundamental.

Los datos precisan protegerse frente a los ataques externos, como el ransomware y frente a pérdidas internas, como los borrados accidentales o malintencionados. La protección y la seguridad de los datos en ambas situaciones son un deseo ferviente de los encuestados.

Los ataques de ransomware pueden no producirse a diario, pero siguen estando en el punto de mira, lo que no es una sorpresa según las tendencias de ransomware que aparecen en las noticias. Si bien la mayoría de los informes describen efectos colaterales, no describen cuáles son sus objetivos, como precaución para que esta información no pueda usarse en ataques futuros.

A pesar de no saber qué puede atacarse específicamente, los encuestados son bien conscientes de que Office 365 pudiera ser el objetivo del ransomware; el 72 % de ellos se mostró preocupado por tales ataques. La preocupación fue mayor en los Estados Unidos (83 %) y menor en EMEA (67 %), con un 73 % en APAC.

Quizás esto no resulte sorprendente, dado que más de la mitad de los encuestados han sido víctimas del ransomware. Las diferencias geográficas también se alinean aquí. Casi dos tercios de los encuestados en los Estados Unidos (64 %) han sido víctimas del ransomware, mientras que un 55 % de los encuestados en APAC y solo un 43 % de ellos en EMEA se han visto afectados por estos ataques. El sufrimiento asociado a verse privado del correo electrónico y otras aplicaciones de colaboración es evidente, en especial con la ampliación del teletrabajo.

Otro factor que aumenta la preocupación en torno al ransomware es la actual tendencia a la exfiltración de datos, en la que se roban los datos antes de bloquearlos y se le revende la información al propietario, o, en los casos en los que el propietario de los datos no quiere pagar, se vende al mejor postor en la web oscura. Las filtraciones de datos de este tipo resultan potencialmente embarazosas y a menudo costosas.

En lo relativo a la protección de datos, la seguridad frente a borrados accidentales o malintencionados es una preocupación mucho más habitual e igualmente inquietante. Casi el 80 % de los encuestados desea múltiples niveles de control de acceso basado en roles para limitar quién tiene acceso a acciones potencialmente dañinas, como el borrado o el purgado de datos.

Me siento preocupado por el bloqueo/ataque de ransomware que tiene como objetivo mis datos de O365.
El 72 % está de acuerdo (n=1793)

Mi organización ha experimentado un ataque de ransomware.
El 52 % está de acuerdo (n=1741)

Para mí es importante disponer de múltiples capas de control de acceso basado en roles para la realización de copias de seguridad.
El 79 % está de acuerdo (n=1828)

Hallazgos clave

HALLAZGO N.º 2

Las organizaciones quieren una restauración detallada y otras funcionalidades que no están disponibles en las capacidades nativas de Microsoft.

Sorprendentemente, solo un tercio de los encuestados ha implementado una solución de copia de seguridad de terceros; el 67 % sigue confiando en la retención y restauración de carpetas eliminadas que incorpora Microsoft, a pesar de la complejidad de esas políticas de retención y la incapacidad de restaurar elementos de forma detallada. Este porcentaje se mostró más alto en los Estados Unidos, con un 74 % de los encuestados que confiaban únicamente en Office 365 para la realización de copias de seguridad. En comparación, solo el 61 % de los encuestados en EMEA y el 70 % en APAC mantienen este planteamiento.

En particular, el 81 % de los encuestados indica que el uso de Teams supone una preocupación en cuanto a la retención de datos. Durante el primer mes completo de la pandemia, por ejemplo, Microsoft informó de un crecimiento del 380 % en el uso de Teams.

Más del 80 % de los encuestados desea una solución de copias de seguridad que cubra Teams y los archivos compartidos. Asimismo, desean que esa solución para Office 365 ofrezca el almacenamiento ilimitado y la posibilidad de descargar una copia de los elementos recuperados.

Según un informe del Grupo de Cumplimiento de Políticas de TI, más de las tres cuartas partes del tiempo dedicado por los departamentos de TI a recuperar algo se debe a un borrado accidental. El aprovechamiento de las carpetas eliminadas existentes y la restauración asistida por Microsoft lleva mucho tiempo, conlleva dificultades y es propenso al fallo; en muchos casos, la restauración de un directorio entero para encontrar un elemento eliminado puede suponer la sobrescritura involuntaria de los datos más recientes y, por tanto, la introducción de nuevos problemas.

Por estas razones, no resulta sorprendente que las copias de seguridad de los datos de Office 365, incluida la recuperación detallada, sean deseables en un alto grado.

Aproximadamente el mismo número indicó que la recuperación de los buzones de correo en otra ubicación o usuario es importante. Esto es algo que no puede hacerse fácilmente con las funciones nativas de Microsoft. Cuando alguien se va de una empresa, termina siendo un usuario eliminado transcurridos 30 días, por lo que esos datos no se pueden guardar en otra ubicación ni en otro usuario.

La facilidad de uso también se aplica al inicio de sesión. En lo que respecta a los servicios de Azure Active Directory y su relación con las nuevas soluciones que instalan las organizaciones, el 76 % de los encuestados afirma que desea una solución que aproveche el inicio de sesión único mediante AAD.

Finalmente, a tres cuartas partes de los encuestados les gustaría poder generar informes diarios sobre todas las copias de seguridad, restauraciones y exportaciones. Si bien esto no parece novedoso, es importante llevar un control de las copias de seguridad. En primer lugar, puede ayudar a proteger los datos al proporcionar una señal temprana de actividad de datos sospechosa en su sistema.

Estoy dependiendo únicamente de las funciones integradas en Office 365 para realizar las copias de seguridad y recuperar los datos de Office 365.
El 67 % está de acuerdo (n=1779)

Para mí es importante contar con la restauración detallada de Exchange, SharePoint, OneDrive y Teams.
El 77 % está de acuerdo (n=1828)

Hallazgos clave

HALLAZGO N.º 3

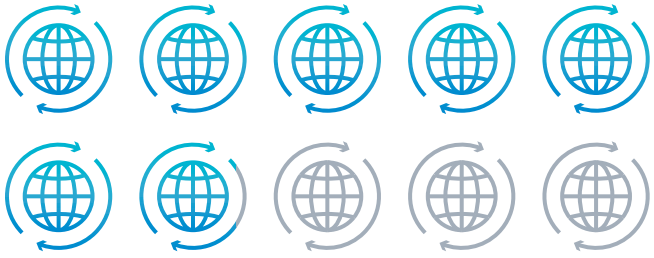
La protección de los datos es una cuestión tanto de seguridad como de conformidad normativa.

Para muchas organizaciones, el lugar donde se almacenen los datos presenta implicaciones de seguridad y cumplimiento normativo. A menudo, los datos incluyen información confidencial, por lo que no solo es preciso mantenerlos seguros, sino que también esa seguridad precisa acogerse a las cuestiones y normativas gubernamentales específicas. También existen legislaciones sobre residencia de datos en diferentes países que regulan el modo en que los datos sobre sus ciudadanos o residentes pueden recopilarse, usarse y almacenarse. Los requisitos pueden incluir plazos para el almacenamiento de los datos y el requisito de que algunos datos deban purgarse a petición.

Las normativas pueden variar según el país, por lo que las organizaciones precisan seguir diferentes requisitos en función del lugar donde operen, lo que no es una tarea fácil para las organizaciones multinacionales. Por ejemplo, dentro de la Unión Europea ciertos tipos de datos confidenciales deben almacenarse en ubicaciones físicas o geográficas específicas.

Casi 7 de cada 10 encuestados muestran su preocupación por este cumplimiento normativo, lo que es comprensible cuando las multas por las infracciones pueden llegar a los 20 millones de euros o a un cierto porcentaje de los ingresos anuales del año anterior, siendo de aplicación la condición con cifras más altas.

Me preocupan los datos cuyas copias de seguridad se efectúan fuera de mi área geográfica (georresidencia).
El 69 % está de acuerdo (n=1787)



Curiosamente, los encuestados de los Estados Unidos son los que más se preocupan (80 %) por las copias de seguridad de los datos fuera de su geografía. En comparación, el 69 % de los encuestados de APAC y el 65 % de los de EMEA afirman que se trata de una preocupación. Esto se debe probablemente a los diversos grados de complejidad para estos requisitos en diferentes zonas geográficas. Por ejemplo, los requisitos son más amplios en Francia y Alemania, mientras que en los Estados Unidos y la India solo se aplican a ciertos sectores o tipos de datos. Los resultados sugieren que en países en los que varían las normas, las personas se sienten más preocupadas porque confían menos en que se manejen correctamente.

El mismo patrón resulta válido para las preocupaciones relacionadas con la privacidad de los datos. Un 85 % de los encuestados de los Estados Unidos está de acuerdo en que es una preocupación, en comparación con el 75 % de los de APAC y el 64 % de los de EMEA que también lo están. Esto sugiere que en países en los que el RGPD lleva asentado varios años, los responsables de TI se sienten más seguros sobre el modo en que están cumpliendo con las legislaciones sobre la privacidad de los datos. En comparación, las normativas sobre privacidad de datos todavía varían de estado a estado en los Estados Unidos, por lo que los responsables de TI probablemente se sienten más preocupados por mantenerse al día con un mosaico de requisitos cambiantes.

Me preocupa el cumplimiento de los requisitos sobre privacidad de datos.
El 73 % está de acuerdo (n=1802)

Hallazgos clave

HALLAZGO N.º 4

Las organizaciones prefieren una solución SaaS que sea rápida y fácil de poner en marcha.

Las organizaciones han mantenido un compromiso de infraestructura consciente y significativo en Office 365 con SaaS y la nube. En cierta forma, se trata de un cambio de perspectiva, ya que las empresas pasan de un enfoque local a soluciones en la nube como Exchange Online, y el crecimiento de Office 365 pone de manifiesto que esta decisión es válida y popular.

Cuando vemos soluciones, no solo los responsables de TI se muestran interesados en las copias de seguridad basadas en SaaS, sino que también tienen la expectativa de una recompensa casi inmediata. Casi 8 de cada 10 desean ser capaces de empezar a ejecutar sus primeras copias de seguridad de inmediato tras iniciar sesión. Otras importantes consideraciones sobre SaaS incluyen la inexistencia de hardware ni software que mantener. Casi tres cuartas partes de los encuestados que respondieron afirmó que se trataba de una consideración de importancia.

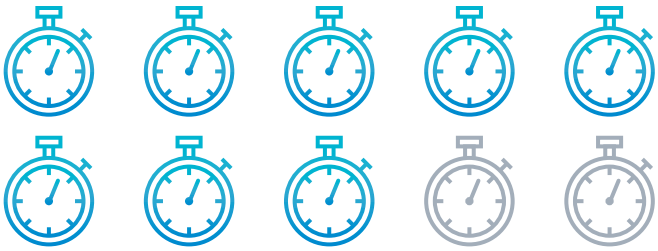
Los encuestados desean mantener sus datos en la nube, y el 77 % indicó que preferiría mantener sus datos de Office 365 en Azure. El rendimiento es parte de la razón, y no resulta sorprendente que el 76 % de estos encuestados también piense que una relación estrecha entre Microsoft y el proveedor de las copias de seguridad resulta extremadamente importante. Los encuestados de los Estados Unidos fueron los más francos en estos dos puntos, con un 83 % y 86 % que estuvo de acuerdo respectivamente.

Los profesionales de la TI también enfatizaron el atractivo de una solución todo en uno en su totalidad, frente a un número de soluciones conocidas que requieren licencias independientes para las copias de seguridad y el almacenamiento en la nube. Además de ser potencialmente más costosas, las soluciones no agrupadas también exigen un mayor mantenimiento administrativo, que es un factor que las organizaciones desean evitar.

Para mí son importantes las copias de seguridad en SaaS para O365, es decir, sin hardware ni software que mantener.
El 74 % está de acuerdo (n=1772)

Para mí es importante una solución simple todo en uno, en lugar de que me obliguen a tener licencias independientes de almacenamiento y capacidad de cálculo.
El 79 % está de acuerdo (n=1787)

Para mí es importante que pueda iniciar sesión y empezar con la ejecución de las copias de seguridad de inmediato.
El 80 % está de acuerdo (n=1805)



Conclusión

Los responsables de TI globales desean una solución SaaS nativa de la nube para Office 365 que sea completa, fácil de usar y sencilla en su puesta en funcionamiento.

La protección de los datos de Office 365 es un requisito en pleno crecimiento, por lo que las organizaciones están buscando soluciones completas y fáciles de usar para las copias de seguridad. El crecimiento de los datos de Office 365 no solo se debe a un número cada vez mayor de usuarios, sino a la naturaleza del teletrabajo que confía en muy alto grado en SharePoint, OneDrive y Teams.

Las organizaciones están fomentando el uso de aplicaciones colaborativas, ya que incrementan la productividad en este entorno y sirven como un registro del trabajo realizado. Sin embargo, este valor se reduce en gran medida sin las copias de seguridad porque la retención nativa de Microsoft no supone una copia de seguridad. Los clientes a menudo consideran que carecen de funciones necesarias para la recuperación, así como la funcionalidad diaria.

Muchas organizaciones descubren que la confianza en estos servicios nativos de retención deja mucho que desear. Los encuestados mostraron una sólida preferencia por la retención detallada, la capacidad de recuperar los buzones de correo de los usuarios en otra ubicación o usuario, y los niveles de control de acceso basado en roles. Más de la mitad de los encuestados desea contar con estas funciones, pero todavía confían en la retención nativa de Microsoft, que no les ofrece ninguna de ellas.

La facilidad de uso es un requisito crucial. La gestión sencilla de las licencias y la instalación rápida hacen incluso más atractiva la decisión de añadir copias de seguridad de terceros y eliminar posibles barreras de entrada. Al mismo tiempo, las preocupaciones por la privacidad de los datos y el cumplimiento normativo ofrecen incentivos adicionales para añadir el tipo adecuado de protección de datos.

Finalmente, la plataforma adecuada que se alinee con su infraestructura existente de Microsoft es otro requisito clave para los profesionales de TI. Muchos se han pasado desde el entorno local de Microsoft, ya que vieron las ventajas que aportaba una plataforma SaaS nativa de la nube. Las ventajas de mantener los datos en la nube para todo el ciclo vital de los datos, incluidos un mejor rendimiento, un inferior coste total de propiedad y ausencia completa de mantenimiento, ilustran la comprensión del valor de la nube.

La facilidad de uso es un requisito crucial. La gestión sencilla de las licencias y la implementación rápida hacen incluso más atractiva la decisión de añadir copias de seguridad de terceros y eliminar posibles barreras de entrada.

Apéndice

HALLAZGO N.º 1

La protección de los datos frente a ataques y pérdidas —tanto de agentes externos como de fuentes internas— es una cuestión fundamental.

Conozco a una organización que ha experimentado un ataque de ransomware y tuvo dificultades con la recuperación.

El 66 % está de acuerdo (n=1758)

HALLAZGO N.º 2

Las organizaciones desean una solución completa de copias de seguridad que sea fácil de usar.

Para mí es importante una solución de copias de seguridad con almacenamiento ilimitado.

El 84 % está de acuerdo (n=1794)

Para mí es importante poder recuperar buzones de correo en otra ubicación o usuario.

El 79 % está de acuerdo (n=1828)

Para mí es importante la posibilidad de descargar una copia de los elementos recuperados.

El 84 % está de acuerdo (n=1792)

Para mí es importante iniciar sesión con servicios de directorios para gestionar mi solución de copias de seguridad.

El 76 % está de acuerdo (n=1797)

Me gustaría disponer de informes diarios sobre mis copias de seguridad, restauraciones y exportaciones.

El 75 % está de acuerdo (n=1828)

HALLAZGO N.º 4

Las organizaciones prefieren una solución SaaS que encaje en la infraestructura que ya están empleando para Office 365.

Para mí es importante tener una solución de copias de seguridad que se ejecute en Azure y almacene los datos de Office 365 en Azure.

El 75 % está de acuerdo (n=1828)

Para mí es importante una relación estrecha entre mi proveedor de copias de seguridad y Microsoft.

El 76 % está de acuerdo (n=1793)

Sobre Barracuda

En Barracuda, luchamos por hacer del mundo un lugar más seguro.

Estamos convencidos de que toda empresa merece disfrutar de soluciones de seguridad en la nube específicas para su labor que sean fáciles de adquirir, instalar y utilizar. Protegemos los correos electrónicos, las redes, los datos y las aplicaciones con soluciones innovadores capaces de crecer y adaptarse a la experiencia de nuestros clientes.

Más de 200 000 organizaciones en todo el mundo confían en Barracuda para su protección —a unos niveles a los que puede que ni ellas sepan que están en riesgo—, de modo que puedan centrarse en llevar su negocio siempre un paso más allá.

Para obtener más información, visite barracuda.com.

Barracuda
Your journey, secured.