

5 criterios para seleccionar una solución de copias para equipos de usuario final



Conseguir una protección eficaz de los equipos corporativos de usuario final entendiendo sus necesidades específicas.

A medida que los trabajadores con manejo de información aumentan, también lo hace el crecimiento – y la importancia – de esos datos finales. Dado que esos datos que se guardan en ese punto final de la cadena, ya sea portátil, ordenador personal, etc..) quedan fuera de la supervisión tradicional de la empresa, son más vulnerables que los datos utilizados en los equipos de oficina. ¿Cómo podemos asegurar esos datos finales para que sean visibles, accesibles y bajo control de la empresa sin afectar a la productividad del usuario y los recursos de red?

Una solución de copia de seguridad diseñada para estos puntos finales corporativos debe proporcionar eficiencia, fiabilidad, y controlar esos datos para garantizar que la productividad se mantenga en todo momento y que la recuperación – ya sea de equipos externos o dispositivos estropeados o no actualizados – sea rápida y fácil, no importa donde esté el equipo: en la empresa, en casa o en un ordenador portátil en cualquier parte del mundo. No hay necesidad de esperar a que el equipo vuelva a la oficina o que los datos sean recuperados en el punto final y llevados a la empresa.

Solo el 8% de los datos de portátiles de empresa actuales, son copiados a servidores gestionados por la empresa.

Fuente: Gartner

Si dispone de copias de seguridad automáticas de un dispositivo, siempre podrá controlar esos datos. Sin copias de seguridad automatizadas, los datos finales se mantendrán fuera de su empresa y por lo tanto, en riesgo de exposición a pérdidas de datos.

Estos son retos importantes, así que es bueno saber que puede proteger fácil y satisfactoriamente los datos del punto final mediante el cumplimiento de cinco sencillos objetivos:

Informe técnico

5 criterios para seleccionar una solución de copias para usuario final

Plan contra errores de los empleados

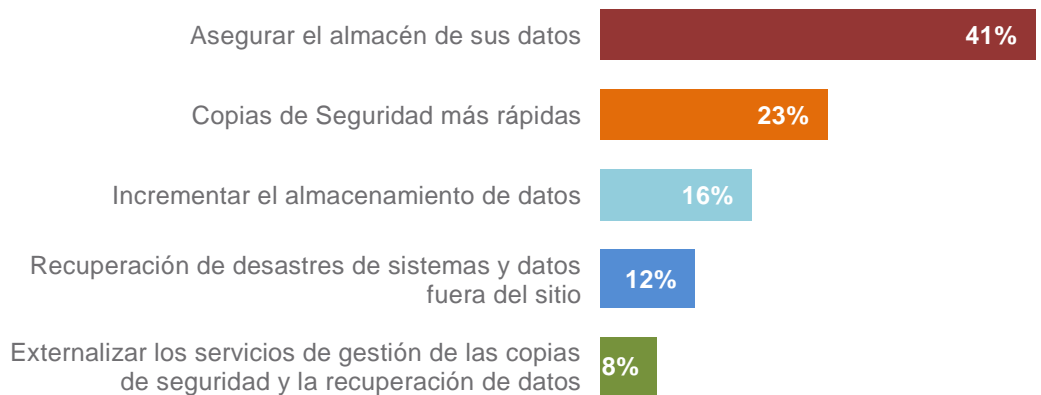
Un mal uso accidental de los datos por parte de los empleados representa un 27% de las violaciones de seguridad. Precauciones simples, como una solución de copia de seguridad empresarial – en lugar de una solución para consumidor final – que almacene los datos de forma segura con dispositivos de localización, cierres del puertos, y la posibilidad de borrar datos ayudan a asegurar los puntos más comunes de fuga de datos.

1. Tenga muy en cuenta las necesidades de los usuarios

Una solución de copia de seguridad para punto final satisfactoria, tiene en cuenta al usuario como primer punto: los usuarios deben tener una experiencia positiva y ver el beneficio de adoptar una solución de este tipo. Por ejemplo, los usuarios de portátiles a menudo trabajan fuera de la oficina a través de redes 3G o WiFi de baja calidad, por lo que el efecto de consumo de la copia en el uso de ancho de banda no es una opción.

- **No resultar invasivo al usuario ni obstaculizar su rendimiento.** Los empleados no pueden ser molestados con detalles de instalación o actualizaciones de software, por lo que estos sistemas no se pueden basar en la participación activa del usuario para garantizar su funcionamiento. En su lugar, se debe optar por una solución que ofrezca despliegues automáticos, configuraciones centralizadas y ejecuciones en segundo plano sin necesidad de participación de los empleados. Una vez hecho esto, delegar selectivamente el control del sistema, para que el usuario, fácilmente, pueda recuperar sus archivos dañados o erróneos en lugar de tener que involucrar al departamento de TI.
- **Parar la copia cuando el ancho de banda es bajo.** Ya sea dentro o fuera, conectado o en modo de hibernación, estos equipos pueden estar siempre en movimiento. Para garantizar que los usuarios no sufren retrasos en situaciones de ancho de banda restringido, considere una función de detección automática de red. Cuando se detecta una conexión WAN limitada, la copia externa se debería detener automáticamente y no reanudarse hasta que el usuario se conecte a una red estándar de nuevo. En tal caso, las copias de seguridad deben seguir en el disco duro del equipo local. También considere una solución de punto final que puede realizar copias de seguridad incrementales basados en la disponibilidad de ancho de banda en lugar de forzar copia de seguridad con ventanas de copia tradicionales que no tienen en cuenta los estados de los dispositivos. Busque una solución que minimice el impacto en la red mediante la utilización de periodos inactivos para la transmisión de los datos.
- **Adapte las copias a sus empleados.** Diferentes usuarios necesitan diferentes políticas de selección de ficheros a copiar y opciones de seguridad, así que necesitará una solución con copias de seguridad basadas en perfiles, lo que permitirá roles de usuario y perfiles de riesgo flexibles. De esta forma podrá realizar numerosos grupos de usuarios con una variedad de políticas de seguridad y respaldo.
- **Ofrecer a los usuarios la restauración de sus archivos, incluso si no están conectados a una red.** Muchas soluciones de protección de puntos final permiten copias de seguridad en dispositivo local además de en la WAN. Esto hace que los archivos respaldados por copia estén disponibles cuando los usuarios están fuera de línea, agilizando la auto-recuperación. Considere la posibilidad de una solución de protección continua de datos, que ofrecen puntos de recuperación frecuentes.

Prioridades de las empresas en trasladarse a sistemas basados en la Nube



Fuente: Vanson Bourne

Informe técnico

5 criterios para seleccionar una solución de copias para usuario final

2. Obtenga lo mejor de ambos mundos: WAN y LAN.

Soluciones híbridas de protección de punto final combinan el propio equipo y el almacenamiento en la nube para ofrecer lo mejor de ambos mundos. La adición de un dispositivo de almacenamiento local le da velocidad LAN junto con la manejabilidad y escalabilidad de la Nube. Acelera el tiempo de protección de copias de seguridad – la copia inicial durará horas en lugar de días – y más rápidas las copias de seguridad y recuperación local. Al servir como "estación de paso" a los datos, esta copia local también aumenta la fiabilidad. Reduzca gastos cuando se transfieren los datos, ya que puede almacenar datos localmente y establecer los tiempos de transmisión basados en la disponibilidad de ancho de banda óptimo y costos. Los resultados: restauración de emergencia rápida, cero impacto WAN, y un lugar seguro para almacenar datos hasta que decida enviarlos a la nube.

Encuesta: ¿Por qué las empresas eligen un sistema híbrido (local / en la Nube) para protección de datos? – Ordenado por industria.

Base: Preguntado a los responsables con una infraestructura de gestión de datos híbrida.	Total	Servicios Financieros	Venta Minorista	Abogados	Seguros	Educación	Gobierno
Incrementar la flexibilidad	74%	72%	84%	90%	79%	72%	55%
Datos más asegurados	61%	54%	54%	30%	68%	67%	64%
Datos protegidos contra desastres naturales y robos	57%	58%	54%	50%	64%	50%	59%
Retención de Copias de seguridad	28%	34%	30%	10%	36%	17%	18%
Bajo Coste	26%	23%	38%	10%	32%	17%	18%
Otros	2%	2%	3%	0%	0%	6%	0%
No sabe / Nocontesta	2%	0%	3%	0%	0%	0%	9%
Base	168	53	37	10	28	18	22

Fuente: Vanson Bourne

Encuesta: ¿Por qué las empresas eligen un sistema híbrido (local / en la Nube) para protección de datos? – Ordenado por región.

Base: Preguntado a los responsables con una infraestructura de gestión de datos híbrida.	Total	UK	FR	DE	NL	USA
Incrementar la flexibilidad	74%	72%	63%	74%	60%	83%
Datos más asegurados	61%	47%	74%	48%	80%	74%
Datos protegidos contra desastres naturales y robos	57%	57%	21%	44%	60%	76%
Retención de Copias de seguridad	28%	16%	21%	19%	50%	44%
Otros	2%	5%	0%	0%	0%	0%
No sabe / Nocontesta	2%	2%	0%	4%	0%	2%
Base	168	58	19	27	10	54

Fuente: Vanson Bourne

Informe técnico

5 criterios para seleccionar una solución de copias para usuario final

3. Despliegue y gestión más fácil con políticas pre-configuradas.

Un despliegue masivo es más fácil cuando las organizaciones utilizan servicios como Microsoft® Active Directory para aprovechar tecnologías existentes y funciones pre-configuradas. Los dispositivos y usuarios se agregan automáticamente utilizando la información de Active Directory y los agentes se instalan silenciosamente cuando los empleados se registran en sus equipos. .

Buscar soluciones con políticas pre-configuradas y adaptadas a las mejores prácticas, para aumentar la velocidad y la facilidad de implementación en los usuarios. Estas políticas pueden especificar detalles como diferentes frecuencias de copia de seguridad, los períodos de retención necesarios, el número de retenciones, la configuración de ancho de banda y los controles de seguridad.

La mayoría de las organizaciones prefieren gestionar de forma global todas las ubicaciones finales de sus usuarios. Una consola de gestión robusta ofrece visibilidad de todos los equipos de su empresa y de todos los sitios, por lo que los datos y sus equipos pueden estar asignados a varios administradores o centros de costos, permitiendo gestionar fácilmente sus funciones y necesidades asociadas.

Una vez que haya identificado las diferentes políticas de usuario, puede utilizar el gestor de configuración para realizar fácilmente las políticas para adaptarse a diferentes perfiles de usuario y gestionar los ajustes personalizados para diferentes variables tales como el cumplimiento con las leyes de protección de datos, leyes internacionales, las excepciones de políticas y de seguridad o configuraciones específicas del sistema operativo.

Se tarda una media de 9 días para que los usuarios sean totalmente operativos después de la pérdida de un ordenador portátil.

Fuente: IDC

4. Centrarse en la economía de almacenamiento.

Una compresión y deduplicación global de los datos a copiar a nivel de bloque, reducirá significativamente su impacto de almacenamiento. Tenga en cuenta que no todos los sistemas de deduplicación de datos usan los mismos métodos y los resultados pueden variar ampliamente. Una solución que combine la deduplicación en el lado del usuario y la compresión con deduplicación en los DataCenters de almacenamiento a nivel mundial, le ahorrará una gran cantidad de almacenamiento y utilización de ancho de banda. Estas características, combinadas con la eficaz copia local, mantiene el impacto WAN al mínimo. .

5. Garantizar la visibilidad de los datos y mantener el control de los mismos.

Una completa protección de los puntos finales asocia cada dispositivo con un empleado: cuando se informa del robo o pérdida de un equipo, usted sabrá exactamente qué datos importantes residen en ese dispositivo remoto y podrá tomar las medidas adecuadas para limitar su riesgo o pérdida de los mismos. Si la copia es utilizada para el cumplimiento legal o para garantizar la productividad y continuidad del negocio, debe ser capaz de realizar un seguimiento y control de esos datos, incluidos los contratos, documentos y correspondencia. Asegúrese de que su solución ofrece esta capa adicional de protección. .

Encuesta: Factores más importantes en soluciones actuales de recuperación de datos.

Base: Preguntado a los responsables con una infraestructura de copias de seguridad de datos híbrida (local y remota)	Total	UK	FR	DE	NL	USA
Fiabilidad al recuperar los datos	43%	33%	46%	53%	37%	48%
Velocidad de acceso a los datos después de un desastre	24%	29%	23%	22%	30%	20%
Los datos están asegurados en el destino	15%	14%	9%	9%	19%	19%
Servicio técnico al usuario final	12%	18%	9%	10%	9%	9%
Pruebas de restauración periódicas	5%	4%	12%	4%	5%	3%
Costo	1%	1%	1%	1%	0%	1%
Base	562	58	19	27	10	54

Fuente: Vanson Bourne

Informe técnico

5 criterios para seleccionar una solución de copias para usuario final

Sin visibilidad de los datos copiados, no se sabe el alcance de las pérdidas ante un desastre o robo y tendrá que tratar cada caso como un “escenario del peor caso”. Una correcta solución de copias de punto final debe darle visibilidad en las variables de copia de seguridad, tales como los tipos de archivo, tamaños de archivo y ubicaciones de almacenamiento asociados. Reconociendo exactamente qué datos residen en un dispositivo, permite tomar decisiones inteligentes en caso de pérdida, robo o fin de vida del dispositivo. Por ejemplo, se puede rastrear rápidamente un dispositivo y borrar de forma remota los datos en caso de robo o pérdida. Si usted ha sufrido una pérdida de datos en el pasado, ya sabrá lo que puede suceder cuando los datos caen en las manos equivocadas y el daño que pueden hacer a la reputación de su empresa. .

Control de prevención de pérdida de datos (DLP – Data Loss Prevention) – Puede añadir valor y mayor seguridad a su solución de copia de seguridad de punto final con medidas DLP fácilmente implementables, cada una de las cuales será de gran valor en caso de pérdida o robo. Estas incluyen la capacidad de rastrear remotamente un dispositivo y borrar sus datos o cerrar los puertos en el equipo para evitar fugas de datos – como una unidad USB – antes de que ocurran.

Se estima un aumento del 44% en el volumen de datos de aquí al 2021.

Fuente: IDC

Asegúrese de que su solución de punto final puede ver los datos vulnerables o que falten en dispositivos rotos, perdidos o con ciclo de vida terminado. Algunas soluciones de copia se aprovechan de “disparadores de tiempo” para activar las tareas de borrado de datos, en lugar de comandos tradicionales de borrado de datos basados en Internet. Esto asegura que los datos de los ordenadores portátiles desaparecidos sean borrados, incluso si el equipo no vuelve a conectarse a Internet.

Encriptación de datos y deduplicación segura – La transferencia de datos por Internet es la principal preocupación de seguridad para la mayoría de las empresas. Cuando se trata de proteger los datos a copiar, su primera consideración debe ser que la encriptación sea con tecnología AES con cifrado de extremo a extremo de 256 bits e integración FIPS 140. Estas normas de seguridad crean barreras significativas contra las violaciones de datos. Para eliminar riesgos, los datos deben ser cifrados con seguridad durante la transmisión y no se tienen que poder descifrar, aunque sea necesario realizar la gestión de deduplicación sobre los mismos. Algunas soluciones no pueden deduplicar los datos sin tener que descifrarlo antes de su almacenamiento en los servidores de destino, dejando sin protección los datos durante ese tiempo. Debe exigir la máxima seguridad a una solución que maneja deduplicación, tanto en el lado del usuario, en el tránsito por Internet, o en el Centro de Datos.

Dé el próximo paso

Para más información sobre los servicios de copias de seguridad y recuperación de JumboCopy, llámenos al 945 148 583, o escríbanos a info@jumbocopy.es o visítenos en www.jumbocopy.es



Continúa Sistemas de Información, S.L.
Central y soporte | C/Castillo de Quejana 9, oficinas 6 y 7 - 01007 Vitoria (Álava)
945 148583
info@jumbocopy.es

EVault y el logotipo de EVault son marcas registradas, y cloud-connected es una marca, y “El mejor caso para el peor caso.”, es una marca de EVault Inc.