



> Lo que necesita saber ya sobre la arquitectura de protección de datos de nueva generación

No necesita que nadie le explique la importancia de una protección de datos eficiente y efectiva. Ya sabe que la capacidad no solo de proteger, sino también de recuperar rápidamente sus datos en caso de interrupciones del sistema y pérdida de datos, es vital para su negocio.

Sin embargo, puede que su arquitectura de protección de datos presente un talón de Aquiles, **y grande**.

Es posible que su hardware e infraestructura vulnerables de computación y red constituyan una base no tan sólida como una roca. Tal vez sea la falta de flexibilidad de los silos de protección de datos lo que anuncia la sentencia de muerte de la eficacia y eficiencia de su plan. En tal caso, la infraestructura se expone a sufrir pérdidas de datos pequeñas y grandes.

Es su responsabilidad identificar todo aquello que posiblemente no funcione y evitar que se produzca cualquier eventualidad.

La buena noticia para usted es que nos encontramos en un momento fascinante por lo que a arquitecturas de protección de datos se refiere. La tecnología está evolucionando a un ritmo exponencial, lo que le permite aumentar la eficiencia operativa, satisfacer mejor las necesidades de sus usuarios finales y ofrecer una protección de datos, deduplicación y recuperación más robustas.

Así que, ¿qué necesita saber sobre el rumbo que está tomando la industria?

Analizaremos las fuerzas impulsoras que hay detrás de estas arquitecturas de protección de datos de rápida evolución, las tendencias que más le conviene conocer, los requisitos que debemos exigir a las arquitecturas de próxima generación y el estado del panorama actual del mercado.

El resto es fácil. Puede que la industria tenga mucho que ofrecer en estos momentos, pero nosotros vamos a resumírselo.

Índice

- Capítulo 1: [¿Qué está motivando los cambios en las arquitecturas existentes?](#)
- Capítulo 2: [Tendencia a tener en cuenta: Dispositivos específicos de protección de datos](#)
- Capítulo 3: [Tendencia a tener en cuenta: Dispositivos de conmutación por error y Cloud-Gateway](#)
- Capítulo 4: [Tendencia a tener en cuenta: Tecnología de protección de datos unificada](#)
- Capítulo 5: [Tendencia a tener en cuenta: Licencias "todo incluido"](#)
- Capítulo 6: [Requisitos para la arquitectura de próxima generación](#)
- Capítulo 7: [El estado del panorama actual del mercado](#)
- Capítulo 8: [Compra de su solución ideal de próxima generación](#)
- Capítulo 9: [Arcserve UDP](#)

¿Qué está motivando los cambios en las arquitecturas existentes?



Para progresar en el mundo actual, los proveedores de protección de datos como Arcserve deben innovar constantemente para ayudar a los clientes a gestionar un grado de complejidad exponencialmente mayor.

¿Qué fuerzas están impulsando el mercado?

Hasta hace muy poco, no había una única solución para la protección de datos, deduplicación y recuperación. Los departamentos de TI se veían obligados a utilizar soluciones de múltiples puntos suministradas por varios proveedores, con lo que se creaban entornos que eran intrínsecamente más complejos y costosos de gestionar.

Estas situaciones, obviamente, también tenían como resultado una protección de datos inconsistente.

Por un momento, plantéese la completa adopción de aplicaciones empresariales de virtualización y multinivel, cada una con su propio patrón complejo de protección de datos. Es suficiente para marearse.

¿Está listo para algo más? ¿Qué hay de la sensibilización de la opinión pública con respecto a la pérdida de datos?

En este ambiente, [los errores en la gestión de los datos difundidos a gran escala](#) tienen un impacto tremendo en la rentabilidad del negocio y la confianza de los consumidores. Por consiguiente, los departamentos de TI se ven forzados a demostrar un cumplimiento riguroso y una gestión adecuada de los datos ante los ejecutivos de primer nivel, consejos de administración e inversores, pero carecen de una predictibilidad de

recuperación consistente y la capacidad de medir los indicadores clave de rendimiento de los que se espera que informen.

Por si eso no fuera suficiente, los departamentos de TI también deben enfrentarse a la consumerización de la TI, al tiempo que trabajan con recursos limitados.

En conjunto puede parecer un desafío insuperable. Pero no lo es.

Se acerca un cambio, y ya iba siendo hora.

En la actualidad, la TI consiste en la interdependencia de sistemas y aplicaciones, todo dentro del contexto de la prestación de servicios.



Los proveedores que han identificado esta oportunidad para irrumpir en el mercado están revisando las mejores prácticas de protección de datos y realizando los cambios fundamentales necesarios para adaptar sus productos. Sus productos de próxima generación ofrecerán más mensurabilidad, una mayor facilidad de uso y mejores capacidades de recuperación para sus clientes.

¿Qué tendencias actuales y futuras debería tener en cuenta?

Tendencia a tener en cuenta: Dispositivos específicos de protección de datos



Los días de comprar, instalar y configurar software de copia de seguridad en nuestros propios servidores están cediendo el paso a una nueva tendencia, una tendencia que promete una vía más sencilla y directa a la protección de datos.

Estamos hablando de dispositivos físicos diseñados específicamente que han sido preconfigurados para ejecutar software de protección y recuperación de datos.

Actualmente, estos dispositivos físicos están muy demandados.

📖 En la actualidad, no solo el 64% de las organizaciones utiliza PBBA en algún punto de sus entornos, sino que otro 29% "tiene previsto" o "está interesado en hacerlo en un futuro inmediato." 📖

– Jason Buffington, Senior Analyst, Enterprise Strategy Group

¿Qué está haciendo aumentar la demanda de dispositivos físicos?

En pocas palabras: **su simplicidad.**

Estas soluciones llave en mano hacen que la arquitectura de protección de datos resulte más fácil de tasar, comprar, configurar e implementar. Eso significa que organizaciones de tamaño pequeño y mediano pueden beneficiarse de capacidades de protección de datos de nivel empresarial sin necesidad de tener departamentos de TI con un gran presupuesto, y con una disponibilidad inmediata de dichas capacidades.

Esto ha acelerado en gran medida la adquisición e implementación de infraestructuras de protección de datos. De hecho, según los datos [publicados por IDC*](#), las compañías gastaron 3260 millones de dólares en dispositivos específicos de copia de seguridad en 2014.

* International Data Corporation (20 de marzo de 2015). Worldwide

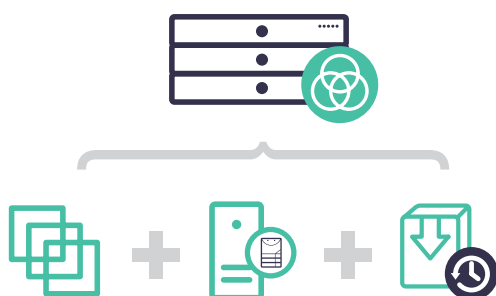
Purpose-Built Backup Appliance (PBBA) Market Revenue Breaks the \$1 Billion Mark in the Fourth Quarter, según IDC [comunicado de prensa]. Obtenido de [aquí](#).

La evolución de los dispositivos físicos de protección de datos

Hasta hace poco, si se adquiría un dispositivo específico de copia de seguridad (PPBA, por sus siglas en inglés) tradicional, se recibía una solución agrupada que incluía software y hardware retroadaptado, una improvisación que carecía de elegancia del diseño, eficiencia y facilidad de uso.

Ahora, el mercado está avanzando hacia soluciones que han sido diseñadas con los dispositivos físicos en mente desde el principio.

Estos dispositivos incluyen:



Dispositivos de copia de seguridad integrados que admiten de forma nativa múltiples aplicaciones y se suministran tanto con software de copia de seguridad como con un servidor.

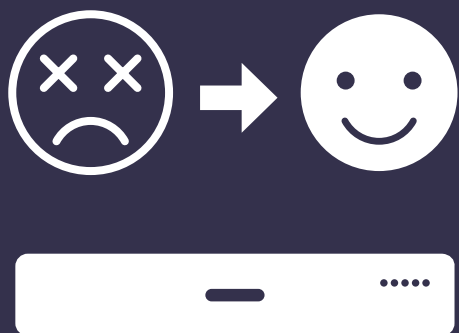


Dispositivos de deduplicación basada en objetivos o más eficiente en el lado del origen que evitan la duplicación de datos y comprimen los datos que quedan, lo que permite reducir la cantidad total de los datos que deben protegerse.

Normalmente, los dispositivos de deduplicación se complementan con dispositivos de copia de seguridad para lograr grandes reducciones de datos. Sin embargo, en la actualidad están apareciendo en el mercado nuevas opciones con capacidades integradas de copia de seguridad y deduplicación en un solo aparato.

Los dispositivos físicos de protección de datos también incluyen dispositivos de conmutación por error y Cloud-Gateway, aunque estos dos productos nativos en la nube son una tendencia emergente en sí misma. Como tal, los analizaremos en mayor profundidad en nuestro siguiente capítulo.

Tendencia a tener en cuenta: Dispositivos de conmutación por error y Cloud-Gateway

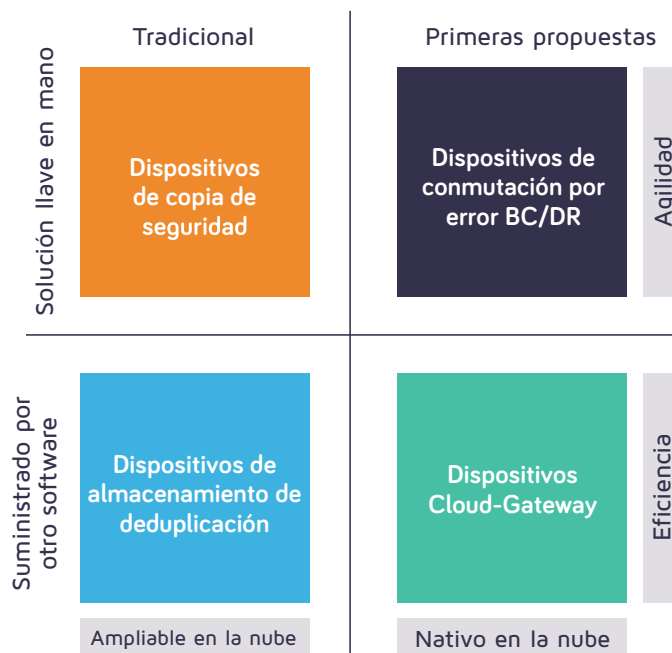


Cuando los profesionales de la industria de la TI hablan sobre dispositivos específicos de protección de datos, suelen referirse a dispositivos de copia de seguridad tradicionales. Ese es el ámbito en que se ha movido el mercado desde hace algún tiempo.

Sin embargo, con el crecimiento exponencial de los datos, que ha hecho aumentar las capacidades de la nube y las expectativas de los usuarios profesionales sobre el acceso a los datos en cualquier momento y lugar, han surgido dos categorías nativas en la nube que representan el camino hacia donde se dirige el mercado.

Se trata de los dispositivos de conmutación por error para copia de seguridad/recuperación ante desastres y los dispositivos Cloud-Gateway.

¿Qué valor aportan estas categorías a su infraestructura de protección de datos?



Fuente: "Data Protection Appliances are better than PBBAs", Jason Buffington, Enterprise Strategy Group, 2014

Dispositivos de conmutación por error para copia de seguridad/recuperación ante desastres

Si su trabajo es caminar por la cuerda floja de la recuperación de datos, entonces considere los dispositivos de conmutación por error para copia de seguridad/recuperación ante desastres su red de seguridad.

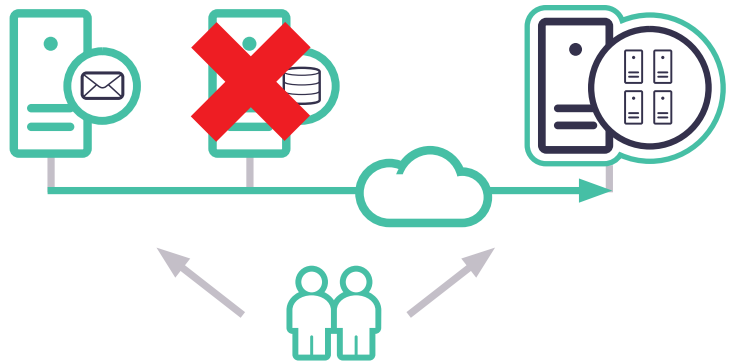
Estos nuevos dispositivos de conmutación por error integran software y hardware diseñados específicamente para ofrecer una alta disponibilidad.

Suelen implementarse localmente, así como en ubicaciones secundarias, de modo que, en el caso de pérdida de datos o fallo del sistema, puede recurrir a una máquina virtual o un servicio dentro del dispositivo, reduciendo así el tiempo de inactividad del sistema y la pérdida de datos.

Es más, la copia de seguridad y recuperación de sus aplicaciones y datos vitales para el negocio son tan fluidas que sus usuarios finales no sabrán que han sido redirigidos a un sitio de recuperación ante desastres.

Estos dispositivos de conmutación por error permiten un alto grado de automatización en el proceso de recuperación de datos, algo que sin duda es de agradecer, y normalmente ofrecen a los administradores de TI y proveedores de servicios gestionados (MSP, por sus siglas en inglés) más valor en relación con los acuerdos de nivel de servicio (SLA, por sus siglas en inglés).

Así que, resumiendo: si su objetivo de tiempo de recuperación es de unos cuantos segundos, le resultará imprescindible este tipo de entorno de recuperación ante desastres.



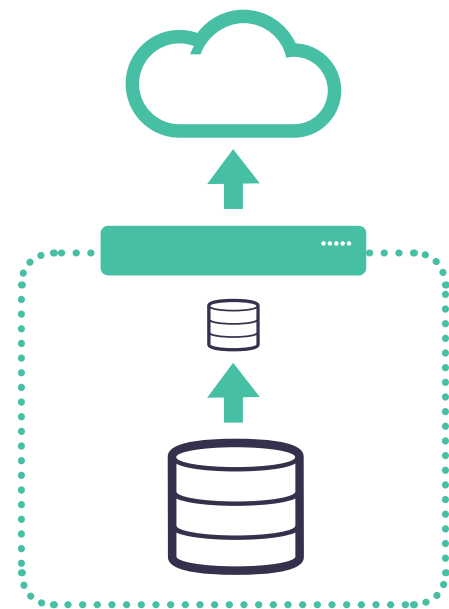
Dispositivos Cloud-Gateway

Los dispositivos Cloud-Gateway son mucho más que una autopista de datos hacia sus MSP o servicio en la nube, ya sea pública o privada. Están diseñados y optimizados de forma nativa para replicar sus datos contenidos en la nube.

¿Cuál es la ventaja?

Aunque no todos los dispositivos Cloud-Gateway están diseñados de la misma forma, ofrecen algunas de las ventajas siguientes o todas ellas.

- Cifrado integrado, que garantiza que sus datos permanezcan seguros
- Almacenamiento local, aunque limitado, que le permite tener acceso inmediato a copias de seguridad recientes almacenadas localmente en la memoria caché de su dispositivo
- Deduplicación, lo que permite reducir el ancho de banda necesario para replicar sus datos al servicio en la nube y lograr un ahorro económico significativo



No cabe duda: a medida que aumente el número de organizaciones que transfieran sus datos a la nube, se incrementará la demanda de estos dispositivos.

Tendencia a tener en cuenta: Tecnología Unified Data Protection



El ejército estadounidense dio en el clavo con su principio de diseño "Keep it simple, stupid" (Hazlo fácil, estúpido).

Por desgracia, las tecnologías de protección de datos no han seguido el principio KISS hasta hace muy poco. ¿Qué entendemos exactamente por protección de datos unificada?

Fundamentalmente, nos referimos a una solución única y sencilla que no solo ofrece todas las funcionalidades necesarias para entornos tanto físicos como virtuales, sino que además ha sido diseñada teniendo en cuenta en todo momento el objetivo final.

¿Qué está motivando la demanda de la tecnología de protección de datos unificada?

Hasta hace muy poco, la protección de datos requería un arsenal de productos de nicho para gestionar el crecimiento exponencial de los datos y la consumerización de IT; productos que no interactuaban entre sí y tenían como resultado silos inflexibles de datos.

Sí, el uso de múltiples soluciones podía satisfacer las necesidades de la organización durante un tiempo, pero a medida que se fuesen añadiendo más soluciones de nicho para responder a una mayor exigencia de las necesidades del negocio y los niveles de servicio, acabaría apareciendo un monstruo de Frankenstein.

Y eso presentaba un desafío único para las pequeñas y medianas empresas.

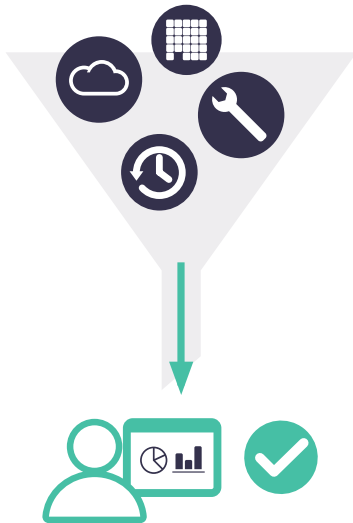
Mientras que las grandes empresas disponían de grandes recursos humanos de TI —talentos en los que se podía confiar que tuvieran conocimientos muy especializados sobre tareas y tecnologías particulares de protección de datos—, las pequeñas y medianas empresas no podían permitirse el lujo de tener enormes departamentos y presupuestos de TI.



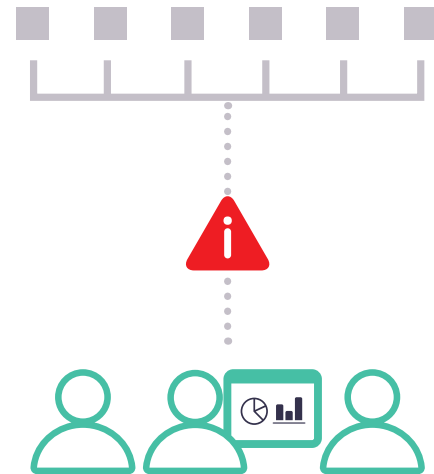
En lugar de eso, debían confiar en generalistas de TI, quienes, ahora, con la ayuda de las tecnologías de protección de datos unificada y un único panel de gestión, pueden implementar capacidades de protección de datos de nivel empresarial; todo a través de una estructura de conocimiento única y común.

Enfoques de los proveedores con respecto a las tecnologías de protección de datos unificada

Si indagamos un poco, descubriremos que los proveedores por lo general han adoptado uno de los dos enfoques principales con respecto a las tecnologías de protección de datos unificada:



Aprovechan los elementos de sus tecnologías básicas de copia de datos, deduplicación, Cloud-Gateway y recuperación y las reinventan para crear una nueva solución unificada en el front-end y el back-end. El resultado final es un producto sencillo e integrado que ofrece todo lo que necesitan en un único lugar y una experiencia de gestión simplificada.



Conectan entre sí paquetes de productos probados de copia de seguridad y recuperación complementarios, accesibles todos a través de un portal único de gestión. Aunque este enfoque permite a los usuarios seleccionar entre una gama más amplia de aplicaciones y el acceso a dichas aplicaciones se realiza a través de una única ubicación, también tiene como resultado una sobrecarga del sistema, lo que no siempre permite la integración y automatización sin problemas de las características, y requiere más recursos gestionados.

Tenga en cuenta que se trata de una tendencia todavía emergente y que el grado de integración de las tecnologías y la madurez de las interfaces de gestión se encuentran en varias fases desarrollo, de modo que sea prudente en sus indagaciones.

Tendencia a tener en cuenta: Licencias "todo incluido"



Licencias "todo incluido":
¿Mito o realidad?

Lo cierto es que esta tendencia tiende a exagerarse. En realidad, solo un número muy pequeño de soluciones disponibles en el mercado son verdaderamente "todo incluido", aunque el mercado está empezando a tomar ese rumbo.

¿Por qué?

En pocas palabras: el precio final resulta confuso. Y, dado que los proveedores desean reducir la confusión de los clientes y ofrecer una experiencia más positiva, están efectuando el cambio.

¿Qué opciones de licencia de software "todo incluido" puede encontrar?

En los casos en que este tipo de licencias existan, pueden basarse en:

- Número de servidores o sockets
- Terabytes de datos protegidos

Y, en los casos en que se basen en la capacidad, esta puede definirse según los datos protegidos antes o después de la deduplicación, lo que puede afectar en gran medida a los costes.

Sin embargo, estas estructuras de precios ayudan a evitar la ambigüedad y a determinar rápidamente qué puede esperar al pagar por la solución que necesita.

¿Qué hay de las licencias sin limitaciones?

Sí, existen, pero son poco habituales, y es posible que el proveedor no sea capaz de suministrarle toda la capacidad que usted desee y con la estructura de precios que necesite, así que evite crearse un presupuesto equivocado.

¿Qué es lo más probable que encuentre en el mercado?

Los proveedores suelen conceder licencias agrupadas de sus características más populares y ofrecer funciones especializadas adicionales como complementos. Esta es una situación que hace que resulte bastante más difícil determinar el precio final.

¿Está planteándose usar dispositivos de copia de seguridad de deduplicación?

En algunos casos, es posible que pague un precio adicional por extras como cifrado, replicación y aceleración de copias de seguridad. Y, en un número reducido de casos, incluso el algoritmo o software de deduplicación representa un complemento que se paga por separado. Se trata de algo que sucede muy a menudo en los paquetes "todo incluido".

¿Está buscando aplicaciones de copia de seguridad integradas que incluyan licencias de software?

Busque bien. Según DCIG*, apenas el 20% de las aplicaciones integradas se suministran con todas las características y funcionalidades que usted necesita. Sí, incluirán software de deduplicación y una consola, pero deberá averiguar si su licencia también incluye replicación, cifrado y software de agente de SO, o si estas características suponen costes adicionales.

Investigue

Independientemente del tipo de licencia que le ofrezcan —limitada o "todo incluido"—, asegúrese de investigar bien y manténgase alerta; puede que la mejor opción de licencia para su organización no sea la que usted considera como primera opción.

Hablando de investigar bien, le animamos a que lea la letra pequeña, en su totalidad.

* * Arcserve (17 de diciembre de 2014). Trends in Data Protection with DCIG [Webinar]. Obtenido de [aquí](#).

Requisitos para la arquitectura de próxima generación

La protección de los datos se está convirtiendo en una tarea cada vez más complicada y algunas de las soluciones que ofrece el mercado se han quedado obsoletas. ¿Cómo puede asegurarse de ser el héroe, no el tonto?

Las arquitecturas de protección de datos de próxima generación son un buen punto de partida. Cuando cumplen con lo prometido, facilitan las cosas, al tiempo que le hacen quedar bien. Son asequibles, completas en lo que a características se refiere y ofrecen un alto grado de escalabilidad.

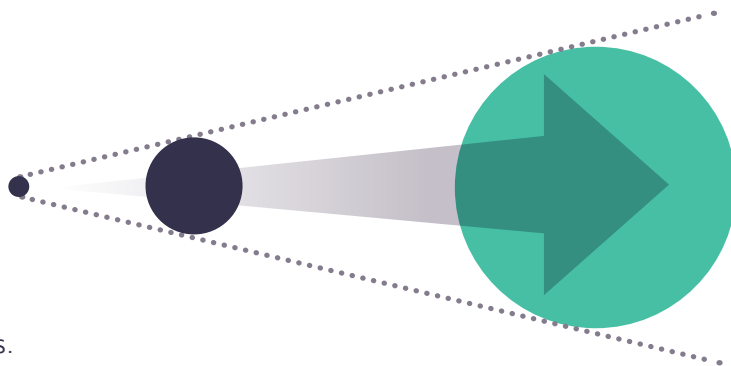
¿Qué cabe esperar a medida que estas soluciones maduren?

Integridad de la solución

Las arquitecturas de próxima generación le ofrecerán todas las tecnologías básicas de protección de datos que necesita en una única solución, incluidas:



En la actualidad, solo algunos proveedores pueden ofrecer de forma satisfactoria soluciones robustas como esta.



Escalabilidad de la solución

Esperamos mucho más de las arquitecturas.

No solo deben adaptarse para manejar volúmenes de datos mayores, al tiempo que cumplir con el objetivo de punto de recuperación (RPO, por sus siglas en inglés), el objetivo de tiempo de recuperación (RTO, por sus siglas en inglés) y los acuerdos de nivel de servicio relativos al rendimiento de las ventanas de copia de seguridad, sino que también deben ser lo bastante flexibles para trabajar en una variedad de plataformas, ya sea disco o cinta, de forma local o remota, en el dispositivo o en la nube.

Y, dado que las organizaciones crecen, se fusionan y son absorbidas, sus arquitecturas de protección de datos deben ser lo bastante modulares y flexibles para ampliarse, sin dejar de ofrecer un alto rendimiento.

¿Qué significa eso en términos sencillos?

Aunque es posible que comience por un software de protección de datos cuya instalación puede realizar usted mismo, a medida que su negocio crezca, seguramente adquirirá un dispositivo y, por último, transferirá parte de sus datos a la nube cuando su organización se consolide.

Una solución altamente escalable le permitirá hacer esas tres cosas cuando y donde lo necesite.

Facilidad de uso de la solución

Las arquitecturas de protección de datos modernas no solo deben ser fáciles de implementar, sino que también deben ser fáciles de usar. Cualquier solución que no pueda ofrecer ese grado de simplicidad sucumbirá ante los productos de la competencia que sí puedan hacerlo.

Busque soluciones que le permitan:

- Unificar diversas tecnologías de una forma que sea fácil de configurar
- Crear planes en base a los indicadores clave de rendimiento de RPO y RTO de una manera tan sencilla como mover un botón
- Permitir tareas y flujos de trabajo complejos que sucedan “entre bastidores”
- Seguir proporcionándole la capacidad para perfeccionar funcionalidades

Asequibilidad de la solución

Hubo una época en que solo las empresas más grandes podían permitirse este nivel de protección de datos y recuperabilidad. De hecho, hasta hace un par de años, la deduplicación y las consolas de gestión unificada eran características reservadas exclusivamente al nivel empresarial.

Eso terminó.

Ahora, las tecnologías de protección de datos son lo bastante flexibles para implementarse de diversas formas, lo que permite optimizar la eficiencia y los gastos operativos, mientras que las licencias las hacen asequibles.



El estado del panorama actual del mercado

Hemos evaluado el estado del panorama del mercado y nos ha parecido deficiente.

La protección de datos comenzó siendo software y ha evolucionado para ofrecer infraestructuras híbridas motivadas por un apetito feroz por los dispositivos y la aparición de la nube como destino.

Dicha evolución ha tenido como resultado productos heredados que ahora resultan obsoletos. Algunos además presentan licencias caras, otros son incapaces de medir las ineficiencias de los procesos. Luego están los que no son escalables o son débiles desde la perspectiva de facilidad de uso. Otros, en cambio, son soluciones nicho que deben añadirse a otras para ofrecer una protección de datos robusta y la recuperabilidad necesaria, lo que agrava el grado de complejidad que debe gestionarse.

En cada uno de estos casos, estas soluciones dificultan su capacidad de prestar de manera consistente un servicio de TI de alta calidad a sus usuarios finales.

¿Cómo puede un proveedor ofrecer una solución que sea realmente de próxima generación?

Para aquellos que se están iniciando en el tema, significa dejar atrás el software heredado y las soluciones retroadaptadas.

Los proveedores progresistas están analizando el panorama actual de protección de datos como un conjunto y están creando tecnologías nuevas e integradas que son altamente flexibles, adaptables y configurables.

¿Qué ofrece actualmente el mercado?

Si está listo para enfrascarse en la búsqueda de una solución, le avisamos: la oferta es muy amplia, y no todos los proveedores han empezado a alinear sus soluciones con las demandas nuevas y exigentes.

Actualmente:



22

proveedores ofrecen 26 soluciones de software de copia de seguridad de servidores virtuales



10

proveedores ofrecen 47 dispositivos de copia de seguridad de deduplicación



14

proveedores ofrecen 72 dispositivos de copia de seguridad integrada

Y estas cifras ni siquiera incluyen los dispositivos de deduplicación y copia de seguridad integrada que también están disponibles como dispositivos virtuales.

Naturalmente, aunque el abanico de proveedores es muy amplio, solo unos pocos lideran el sector

Estos son:

- Arcserve® UDP
- CommVault® Simpana®
- Dell® AppAssure
- Symantec Backup Exec™
- UniTrends™
- Veeam®

Con multitud de proveedores ofreciendo tantas soluciones al mercado, puede resultar difícil encontrar la solución adecuada de protección de datos.

Sin embargo, es una tarea que merece la pena llevar a cabo.

Cuando encuentre una arquitectura de próxima generación que ofrezca integridad, escalabilidad y facilidad de uso de la solución, estará preparado para enfrentarse a sus desafíos actuales en materia de datos, y al mismo tiempo conseguirá mejorar la eficiencia.

Compra de su solución ideal de próxima generación



Cuando estudie la gama de opciones disponibles en el mercado e indague en las características y las funcionalidades que ofrecen cada una de ellas, se dará cuenta de que comparar los diversos productos es una tarea muy pesada.

Dicha tarea resulta especialmente complicada cuando los proveedores no son lo bastante claros sobre las características que están o no están incluidas en el precio anunciado.

Así que, ¿qué debería tener en cuenta cuando estudie las diversas opciones?

Olvídese del bombo publicitario y decida qué características necesita.

Asegúrese de preguntar:

- Si la solución está disponible como dispositivo físico, virtual o ambos.
- ¿ Ofrece la solución una consola de gestión unificada?
 - De ser así, ¿en qué punto del proceso de desarrollo se encuentra el proveedor?
 - ¿En qué grado se integra dicha consola con los diversos dispositivos que debe gestionar?
 - Antes de firmar un contrato, asegúrese de probar la integración o ver una demostración para comprobar que la solución cumple con sus expectativas.
- ¿Incluye la solución un dispositivo Cloud-Gateway que permite copia de seguridad, almacenamiento de datos y recuperación en la nube?
- Si la deduplicación es una de las características de la solución, ¿está en el lado del destino, en el lado de la fuente o en ambos?
- ¿Incluye la solución dispositivos de conmutación por error para copia de seguridad/recuperación ante desastres y restauraciones inmediatas?

Con respecto a la licencia, asegúrese de leer la letra pequeña. Detenidamente

Formule preguntas como:

- ¿Se trata de una licencia “todo incluido”? De ser así, ¿puede el proveedor cumplir realmente con lo prometido?
- ¿Se trata de una licencia agrupada con limitaciones? De ser así, ¿cuál es el precio final después de añadir las funciones especializadas necesarias?



¿Qué debería tener en cuenta?

Le recomendamos que preste especial atención a los aspectos que las arquitecturas de protección de datos de próxima generación pueden (y deberían) ofrecer.

Estos son:

- Integridad de la plataforma: un único punto para todas sus necesidades de protección de datos
- Tecnologías unificadas: perfecta integración de todos los componentes, lo que evita la creación de silos impenetrables
- Virtualización: máquinas virtuales que le permiten ejecutar varios sistemas operativos y aplicaciones en un único servidor físico
- Facilidad de uso: diseño orientado al cliente que permite a los generalistas de IT implementar y gestionar la solución
- Conmutación por error inmediata/BMR: alta disponibilidad y recuperación ante desastres que garantizan la continuidad del negocio
- Replicación: mayor tolerancia a fallos mediante la replicación de datos automatizada
- Cinta/Archivo: admite la replicación a cinta para garantizar una mayor fiabilidad
- Reducción de datos: deduplicación basada en objetivos o más eficiente en el lado del origen que reduce la cantidad total de los datos que deben protegerse
- Servicio en la nube: capacidad mejorada para transferir los datos a la nube y gestionarlos

¿Quiere saber qué resultados ofrecen las mejores marcas?

	Arcserve UDP 8000	CommVault	Dell	Unitrends	Veeam
INTEGRIDAD DE LA PLATAFORMA					
Unificación					
Virtualización					
Facilidad de uso					
Conmutación por error inmediato/ BMR					
Replicación					
Cinta/Archivo					
Reducción de datos					
Servicio en la nube					

Ninguno
 Básico
 Medio
 Advanced
 Mejor

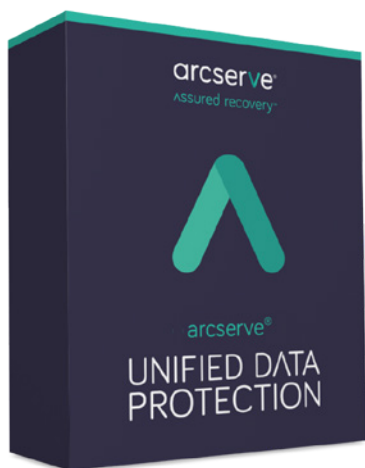
Fuente: Arcserve

Naturalmente, no hay ninguna solución adecuada para todas las organizaciones, de modo que averigüe los requisitos de su arquitectura y estudie detenidamente las diversas opciones para encontrar la solución adecuada.

Arcserve UDP

Su reputación está en juego. ¿Hasta qué punto desea que decida el azar?

Gracias a la nueva generación de dispositivos de protección unificada de datos de Arcserve (o UDP de Arcserve), podrá utilizar la solución de protección de datos más completa de la industria, con capacidades de recuperación asegurada (Assured Recovery™) y almacenamiento en la nube.



¿Qué incluye?

Arcserve UDP alivia algunas de las presiones de su complicado trabajo con ventajas como:

- ✓ **Una arquitectura de protección de datos y recuperación simplificada que le permitirá instalar el dispositivo y olvidarse.**
- ✓ **Una protección de datos y sistemas significativamente mejor, así como opciones de recuperación en soluciones heredadas**
- ✓ **Grandes mejoras en la eficiencia operativa y reducción de costes**

¿Qué ofrece Arcserve UDP?

Arcserve UDP ofrece un software completo llave en mano de protección de datos y recuperación que incluye capacidades de copia de seguridad, replicación y deduplicación global. Además Arcserve UDP cuenta con la consola de gestión más unificada de la industria y la solución de protección de datos basada en imágenes mejor integrada del mercado.

Arcserve UDP también ofrece:

- ✓ Tecnologías de conmutación por error para copia de seguridad/recuperación ante desastres de alta disponibilidad, incluidas capacidades para proteger tres máquinas virtuales en espera
- ✓ Capacidad de software en la nube que le permite replicar sin esfuerzo los datos en servicios de nube públicos y privados y en MSP
- ✓ Protección de servidores físicos y virtuales: la única solución de software unificado del mercado que lo hace.
- ✓ Software que ofrece pruebas automatizadas de recuperación ante desastres de sistemas, aplicaciones y datos vitales para el negocio; todo sin generar periodos de inactividad ni afectar a los sistemas de producción
- ✓ Licencia de software "todo incluido" basada en los sockets de la CPU (físicos o virtuales) o en los terabytes de datos protegidos