

## Cyber Recovery con servicios de datos de múltiples nubes para Dell EMC PowerProtect

### Servicio de Cyber Recovery habilitado para múltiples nubes

#### Confiable y seguro

- Entorno de vault aislado de forma física y lógica, desconectado de las redes corporativas gracias a una brecha de aire operativa
- Copias inmutables de los datos en un vault seguro fuera de instalaciones para mantener la integridad de datos
- El análisis inteligente ofrece aprendizaje automático e indexación de contenido completo dentro del vault

#### Rentable

- Infraestructura de vault principal entregada como servicio
- Conexión directa disponible de alto ancho de banda y baja latencia para proveedores de servicio en la nube pública
- Nada de tarifas de egreso de Microsoft Azure y Oracle Cloud

#### Conveniencia sin sacrificios

- Proteja los datos cruciales que residen en la nube o en las instalaciones
- Restablezca los datos para cualquier proveedor de servicio en la nube pública sin inconvenientes
- Obtenga la flexibilidad y la conveniencia de la nube sin sacrificar la seguridad

### Protección cibernética para las implementaciones en las instalaciones y en la nube

Cada minuto de cada día, el ransomware y otros ataques cibernéticos sofisticados amenazan con robar o comprometer el activo más crucial de una empresa: sus datos. Esto puede ocasionar pérdidas de ingresos, daños a la reputación y costosas multas normativas. Es clave proteger los datos cruciales y recuperarlos con integridad de datos validada para poder reanudar las operaciones comerciales normales después del ataque.

Los entornos híbridos y de múltiples nubes ofrecen flexibilidad operativa, posibilidad de escalar rápidamente y acceso a servicios y hardware innovadores. Sin embargo, el enfoque en la dispersión y duplicación de datos en múltiples nubes puede conducir a nuevos riesgos de seguridad y cumplimiento, posibles problemas de sincronización y mayores costos de recursos. Este enfoque también puede reducir la visibilidad en los distintos entornos, lo que ocasiona que la protección sea insuficiente contra las amenazas cibernéticas en evolución de hoy en día. Es necesaria una mejor manera de que sus datos sean accesibles simultáneamente para los proveedores de servicio en la nube pública sin comprometer la seguridad, a la vez que conserva la libertad de elegir cualquier proveedor de servicio en la nube y evita la dependencia de proveedores.

A medida que mueve más cargas de trabajo y datos a la nube, es imprescindible invertir en una solución de protección cibernética para los datos cruciales, dondequiera que se encuentren. Dell Technologies ofrece un vault de datos seguro y análisis inteligentes que protegen sus datos cruciales contra ataques cibernéticos, ransomware y amenazas internas.

### Cyber Recovery habilitado para múltiples nubes

Es sencillo configurar un vault de Cyber Recovery con servicios de datos de múltiples nubes para Dell EMC PowerProtect, con tecnología de Faction. Este servicio seguro de vaulting de datos brinda un vault con una brecha de aire lógica que se basa en la infraestructura segura y habilitada para múltiples nubes que protege los datos cruciales contra los ataques cibernéticos. Si la recuperación de datos es necesaria, puede optar por restaurar sus datos desde su vault a AWS, Microsoft Azure, Google Cloud, Oracle Cloud o volver a su entorno en las instalaciones.

Los análisis inteligentes de CyberSense están completamente integrados con este servicio de Cyber Recovery y adoptan un enfoque único para descubrir los ataques cibernéticos, observar cómo los datos cambian con el tiempo y usar los análisis para detectar indicios de corrupción debido al ransomware. Esto proporciona una capa adicional de seguridad al validar la integridad de los datos protegidos fuera de instalaciones dentro del vault de Cyber Recovery.

### Cyber Recovery con servicios de datos de múltiples nubes para Dell EMC PowerProtect Arquitectura segura

El entorno de vault seguro incluye un sistema de servicios de datos de múltiples nubes para Dell EMC PowerProtect a fin de que sirvan como el destino de replicación de sus sistemas principales de Dell EMC PowerProtect DD o Dell EMC PowerProtect DD Virtual Edition (DDVE). Los recursos informáticos dedicados ejecutan las herramientas de administración de Cyber Recovery y cualquier herramienta de análisis de CyberSense. En combinación con la seguridad física y el aislamiento del vault, esta solución incluye una brecha de aire operativa: esta brecha de aire permite acceder al vault solo el tiempo necesario para poder replicar los datos desde el sistema principal e, incluso en ese instante, el acceso es muy limitado. En cualquier otro momento, el vault estará desconectado del entorno de producción del cliente. Las copias inmutables de los datos que selecciona el usuario se crean en el vault de Cyber Recovery alojado en un centro de datos de Faction. Una vez que se encuentra la copia de los datos seleccionados dentro del vault seguro y aislado, los

datos no se pueden modificar, eliminar o cambiar de otra manera durante una duración prescrita. Los análisis de CyberSense, con su aprendizaje automático y las funcionalidades de indexación de contenido completo, analizan cada conjunto de datos dentro de la seguridad del vault.

### Protección de los servicios existentes de datos de múltiples nubes para las implementaciones de Dell EMC PowerProtect

Si se combina con los servicios de datos de múltiples nubes para Dell EMC PowerProtect, los clientes logran una protección de datos soberana en todas las nubes (AWS, Google Cloud, Oracle y Azure) y, por lo tanto, pueden proteger sus datos cruciales dentro de un vault seguro de Cyber Recovery.

Los servicios de datos de múltiples nubes para Dell EMC PowerProtect se pueden utilizar como un sistema multipropósito: un destino de respaldo para los datos de aplicaciones nativas en la nube o un destino de replicación para los sistemas de PowerProtect existentes. El vault de Cyber Recovery es una opción adicional que se puede agregar fácilmente para brindar aislamiento de los datos cruciales contra los ataques cibernéticos y validación de la integridad de datos.

### Protección de datos en las instalaciones del cliente

Los clientes pueden replicar los datos desde PowerProtect DD en las instalaciones a un vault de Cyber Recovery en uno de los centros de datos de Faction. Esto les brinda a las empresas la

mejor oportunidad posible de recuperación cuando sus respaldos principales o de producción se ven comprometidos o si su ubicación de DR se ve vulnerada o infectada. Si se produce un ataque cibernético, podrán identificar rápidamente la copia limpia más reciente de los datos dentro del vault de Cyber Recovery remoto y recuperar sus sistemas cruciales en las instalaciones u optar por recuperarlos en la nube si su servicio se diseñó para este movimiento de recuperación.

### Protección de datos en la nube pública

Para las aplicaciones nativas en la nube que ya utilizan PowerProtect DDVE (un destino de respaldo virtual en la nube compatible con AWS, Google Cloud y Azure), el servicio del vault de Cyber Recovery es un servicio opcional que permite a los clientes replicar sus datos cruciales en un vault seguro.

### Dell EMC PowerProtect Cyber Recovery con CyberSense

PowerProtect Cyber Recovery es la primera solución que integra completamente CyberSense, lo que agrega una capa inteligente de protección que facilita la búsqueda de corrupción de datos cuando un ataque penetra en el centro de datos. Este enfoque proporciona una indexación de contenido completo y utiliza el aprendizaje automático para analizar más de 100 estadísticas basadas en contenido y detectar indicios de corrupción debido al ransomware. CyberSense detecta la corrupción con hasta un 99,5 % de confianza, lo que ayuda a identificar las amenazas, diagnosticar los vectores de ataque y, al mismo tiempo, proteger el contenido crucial de la empresa, todo dentro de la seguridad del vault.

### Soluciones de protección de datos de Dell Technologies: lidere el camino hacia la nube

Puede proteger sus datos cruciales en la nube sin comprometer la integridad, la confidencialidad ni la disponibilidad. Cyber Recovery con los servicios de datos de múltiples nubes para Dell EMC PowerProtect protege con confianza sus datos cruciales desde un único destino, independientemente de si están alojados en la nube o en las instalaciones. Para obtener más información, comience aquí.

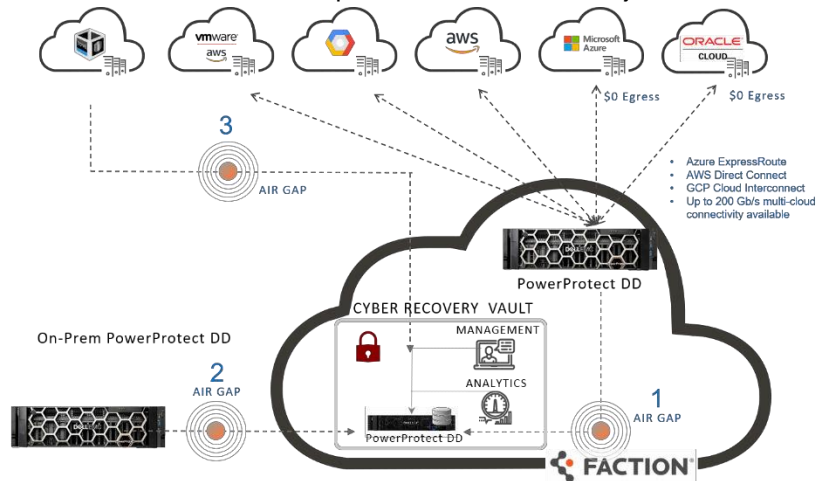


Figura 1: casos de uso de los servicios de datos de múltiples nubes para Dell EMC PowerProtect

1. Protección de los servicios existentes de datos de múltiples nubes para las implementaciones de Dell EMC PowerProtect
2. Protección de datos en las instalaciones del cliente
3. Protección de datos en la nube pública



[Obtenga más información](#) sobre Cyber Recovery con los servicios de datos de múltiples nubes para Dell EMC PowerProtect



[Comuníquese](#) con un experto de Dell Technologies



[Obtenga más información](#) sobre las soluciones de protección y respaldo de datos en la nube

