Recuperación cibernética con Servicios de Datos Multicloud para Dell PowerProtect

Powered by:

DELL Technologies

ARROW

Servicio de recuperación cibernética habilitado para múltiples nubes

Confiable y Seguro

- Entorno de vault aislado físico y lógicamente, desconectado de las redes corporativas a través de un espacio de aire operativo.
- Copias de datos inmutables en un vault seguro fuera de las instalaciones que mantiene la integridad de los datos.
- El análisis inteligente proporciona M/L e indexación de contenido completo dentro del vault.

Económico

- Infraestructura central de vault entregada como un servicio.
- Conexión directa disponible de alto ancho de banda y baja latencia a proveedores de nube pública.

Conveniencia sin compromiso

- Proteja los datos críticos que residen en la nube o en las instalaciones.
- Restaure datos a cualquier proveedor de nube pública sin problemas.
- Obtenga la flexibilidad y la comodidad de la nube sin comprometer la seguridad.

Protección cibernética para implementaciones locales y en la nube

Cada minuto de cada día, el ransomware y otros ciberataques sofisticados amenazan con robar o comprometer el activo más crítico de una empresa: sus datos. Esto puede conducir a la pérdida de ingresos, daños a la reputación y multas regulatorias costosas. Proteger sus datos críticos y recuperarlos con integridad de datos validada es clave para reanudar las operaciones comerciales normales después del ataque.

Los entornos híbridos y de múltiples nubes ofrecen flexibilidad operativa, la capacidad de escalar rápidamente y acceso a servicios y hardware innovadores. Sin embargo, el enfoque de dispersión y duplicación de datos en múltiples nubes puede generar nuevos riesgos de seguridad y cumplimiento, posibles problemas de sincronización y mayores costes de recursos. Este enfoque también puede reducir la visibilidad en sus diversos entornos, lo que lleva a una protección insuficiente contra las amenazas cibernéticas en constante evolución.

Se necesita una mejor manera de hacer que sus datos sean accesibles simultáneamente para los proveedores de nube pública sin comprometer la seguridad, conservar su libertad para elegir cualquier proveedor de nube y evitar el bloqueo de proveedores.

A medida que mueve más cargas de trabajo y datos a la nube, es imperativo invertir en una solución de protección cibernética para datos críticos, donde sea que se encuentren sus datos. Dell Technologies ofrece un vault de datos seguro y análisis inteligente que protege sus datos críticos de ataques cibernéticos, ransomware y amenazas internas.

Recuperación cibernética habilitada para múltiples nubes

Configurar un vault de recuperación cibernética con servicios de datos de múltiples nubes para Dell PowerProtect, con tecnología de Faction, es simple. Este servicio seguro de vault de datos es un vault lógicamente aislado construido sobre una infraestructura segura habilitada para múltiples nubes que protege sus datos críticos de los ataques cibernéticos. Cuando se requiere la recuperación de datos, puede optar por restaurar sus datos desde su vault a AWS, Microsoft Azure,Google Cloud, Oracle Cloud o volver a su entorno local.

El análisis inteligente de CyberSense está completamente integrado con este servicio de recuperación cibernética y adopta un enfoque único para descubrir ataques cibernéticos, observando cómo cambian los datos con el tiempo y utilizando análisis para detectar signos de

corrupción debido al ransomware. Esto proporciona una capa adicional de garantía al validar la integridad de los datos protegidos dentro de las instalaciones dentro del Cyber Recovery Vault.

Recuperación cibernética con servicios de datos multicloud

El entorno vault seguro incluye servicios de datos de nube múltiple para el sistema Dell PowerProtect que sirve como destino de replicación para sus sistemas principales Dell PowerProtect DD o Dell PowerProtect DD Virtual Edition (DDVE).

Los recursos de cómputo dedicados ejecutan las herramientas de Cyber Recovery Management y cualquier herramienta de análisis de CyberSense. En combinación con la seguridad física y el aislamiento del vault, esta solución incluye un espacio de aire operativo: este espacio de aire permite el acceso al vault solo el tiempo suficiente para replicar los datos del sistema principal e, incluso entonces, el acceso está severamente limitado. El resto del tiempo, el almacén está desconectado del entorno de producción del cliente. Se crean copias inmutables de los datos seleccionados por el usuario en el Cyber Recovery Vault alojadas en un centro de datos de Faction. Una vez que una copia de los datos seleccionados está segura,los datos no pueden ser alterados, eliminados o cambiados durante un período prescrito. El análisis de CyberSense, con sus capacidades de indexación de contenido completo y aprendizaje automático, puede analizar cada conjunto de datos dentro de la seguridad del vault.

Protección para servicios de datos de multicloud existentes para implementaciones de Dell PowerProtect

Cuando se combina con los servicios de datos multicloud para Dell PowerProtect, los clientes logran una protección de datos soberana en todas las nubes (AWS, Google Cloud, Oracle y Azure) y luego pueden proteger sus datos críticos dentro de un vault de recuperación cibernética segura. Los servicios de datos de múltiples nubes para Dell PowerProtect se pueden usar como un sistema multipropósito: un destino de respaldo para los datos de aplicaciones nativas de la nube o un destino de replicación para los sistemas PowerProtect existentes.

El vault de recuperación cibernética es una opción adicional que se puede agregar fácilmente para proporcionar aislamiento de datos críticos de ataques cibernéticos y validación de la integridad de los datos.

Protección de datos en las instalaciones del cliente

Los clientes pueden replicar datos desde un PowerProtect DD local al Cyber Recovery Vault en uno de los centros de datos de Faction. Esto le da a las organizaciones la mejor oportunidad posible de recuperación cuando su producción o las copias de seguridad primarias se han visto comprometidas o su ubicación DR ha sido violada o infectada.

Si se produce un ataque cibernético, pueden identificar rápidamente la copia limpia más reciente de los datos dentro del Cyber Recovery Vault y recuperar sus sistemas críticos en las instalaciones u optar por recuperarse en la nube si su servicio se ha diseñado con este movimiento de recuperación.

Protección de Datos en la Nube Pública

Para las aplicaciones nativas de la nube que ya usan PowerProtect DDVE (un objetivo de copia de seguridad virtual en la nube compatible con AWS, Google Cloud y Azure), el servicio de Cyber Recovery Vault es un servicio opcional que permite a los clientes replicar datos críticos en un vault seguro.

Soluciones de protección de datos de Dell Technologies: liderando su camino hacia la nube

Puede proteger datos críticos en la nube sin comprometer la integridad, la confidencialidad o la disponibilidad. La recuperación cibernética con servicios de datos de múltiples nubes para Dell PowerProtect protege sus datos críticos sin importar si están alojados en la nube o en las instalaciones desde un único destino con confianza. Para obtener más información, comience aquí.

Descubra más en:
www.moderndatacenter.es