RESUMEN DE LA SOLUCIÓN

Defensa de los datos con InfiniBox®: Sea cual sea la amenaza (ransomware, desastres naturales, fallos del sistema o errores humanos), InfiniBox le cubre las espaldas.

EL DESAFÍO

Actualmente, los datos residen en un mundo más peligroso que nunca. Los desastres naturales son cada vez más frecuentes, y un simple error humano puede dejar inutilizados por completo volúmenes enteros de sus valiosos datos. A ello se añade la ciberdelincuencia actual, como el ransomware y el malware, que encabeza la lista de preocupaciones de los directores generales y de los responsables de información y seguridad.

Por muy dramático y peligroso que suene todo esto, la realidad es así, o puede serlo si no está preparado. Para proteger sus datos frente a estas amenazas, la mayoría de las empresas recurren a la protección de datos clásica (copias de seguridad). Además, muchas aplican una planificación de continuidad de negocio, que mantiene la fiabilidad y la disponibilidad de sus datos a pesar de las interrupciones y de los ataques. Esta planificación se complica aún más debido al auge de los ataques de ransomware y malware.

Ni siquiera las organizaciones más sofisticadas saben nunca con seguridad si sus datos están suficientemente protegidos. Para asegurarse de disponer de lo último en protección de datos moderna, incluyendo la resiliencia de los datos y la ciberresiliencia, InfiniBox e InfiniBox SSA de Infinidat ofrecen la arquitectura de referencia InfiniSafe®, que le permite establecer los procesos adecuados con las herramientas y tecnologías adecuadas para ayudarle a mantener la seguridad, la disponibilidad y la fiabilidad de sus datos.

En este resumen de la solución, analizaremos una de las amenazas más comunes y graves a la que se enfrentan los datos: la ciberdelincuencia y el ransomware.

> *«...la ciberdelincuencia se ha convertido en un asunto tan grave que, en las recientes encuestas a directores generales realizadas por la revista Fortune en mayo de 2021 y por KPMG en marzo de 2021, los participantes mencionaron los riesgos de la ciberseguridad como la amenaza número 1 para sus negocios.»*

La ciberdelincuencia está aumentando de forma exponencial

- No hay que preguntarse SI seré atacado, sino CUÁNDO y con qué frecuencia podría suceder. Hoy en día es algo inevitable y todas las empresas deben estar preparadas.
- La ciberdelincuencia no se limita a un único tipo de ataque. Algunos de los ataques más populares son los ataques de phishing o suplantación de la identidad, el robo de IP en línea y los fraudes por Internet (como el del consabido Secretario General de las Naciones Unidas que ofrece decenas de millones de dólares al afortunado destinatario).
- Los ataques de malware sofisticados, como la amenaza persistente avanzada (APT), necesitan más recursos para perpetrarse, pero los resultados compensan. Los hackers que emplean la APT se dirigen a redes con gran cantidad de datos valiosos, suficientes recursos y la posibilidad de sufrir una enorme humillación pública si el ataque prospera.[1]
- De hecho, la ciberdelincuencia se ha convertido en un asunto tan grave que, en las recientes encuestas a directores generales realizadas por la revista Fortune en mayo de 2021[2] y por KPMG en marzo de 2021[3], los participantes mencionaron los riesgos de la ciberseguridad como la amenaza número 1 para sus negocios.
- Está bien documentado que los ciberataques se ejecutan con meses de planificación. El tiempo medio de permanencia supera los 9 meses en que los intrusos se infiltran en el entorno de una empresa.

Ransomware

El ransomware es una forma de malware. Sin embargo, a diferencia de los ataques APT de alto riesgo y con grandes beneficios, los hackers

[1] «Qué es un APT (Advanced Persistent Threat)?» Kaspersky
[2] «Fortune 500 CEO survey»
[3] «KPMG 2021 CEO Outlook Pulse Survey»
[4] «Revealed: The Supermarkets that Will Sell You Malware for $50» Forbes

INFINIDAT

pueden comprar el ransomware «listo para usar» en la web oscura o dark web. Muchos de estos ataques son económicos, y algunos vendedores emprendedores llegan incluso a alquilar ransomware, lo que ha dado lugar a la ciberdelincuencia como servicio (CaaS).[4]

Los ataques de ransomware introducen software que cifra automáticamente todos los archivos y volúmenes a los que puede acceder. Si el ransomware ataca un ordenador conectado en red, el proceso de cifrado se extenderá por la red, lo que afectará a todo el almacenamiento primario y secundario, incluyendo copias de seguridad y archivos. A menudo, el almacenamiento secundario constituye el primer objetivo, lo que limita su capacidad de recuperar la información y refuerza la posición del intruso. A continuación, los hackers solicitan un pago a las víctimas para comunicarles la clave de descifrado.

¿Por qué no debe pagar el dinero?

Muchas víctimas prefieren pagar el rescate y confiar en obtener la clave antes que perder sus datos por completo.

Esta decisión es un gran error. El informe **«State of Ransomware 2021»** de Sophos reveló los resultados de su investigación en torno a los incidentes de ransomware: El 92 % de las organizaciones que pagó un rescate en los últimos 12 meses no recuperó la totalidad de sus datos. La cantidad media de datos recuperados en el caso de todos los encuestados fue del 65 %, lo que significa que algunos de ellos recuperaron la información parcialmente; otros, por completo; y otros, nada en absoluto. El informe de Sophos también puso de manifiesto que el coste medio del recovery en la primera mitad de 2021 ya había duplicado al de 2020. En definitiva, el coste del recovery puede ascender a millones de dólares.

> *«Me ha impresionado mucho el rendimiento, la rentabilidad y la gestión del sistema que OFFSITE ha implementado. La funcionalidad de snapshots inmutables [de Infinidat] ha supuesto un gran valor añadido para proteger los datos contra el ransomware».*
>
> - **Director de Tecnología**, OFFSITE

Asimismo, los gobiernos de todo el mundo están elaborando normas, reglamentos y leyes relativas al pago de rescates y a la denuncia de incidentes. En este sentido, resulta importante que las empresas estén al corriente de los requisitos de sus respectivas regiones.

LA SOLUCIÓN

El potente sistema de almacenamiento de Infinidat, InfiniBox, ofrece una solución basada en la inteligencia artificial de tipo «instalar y olvidarse» con un 100 % de disponibilidad sin precedentes, un rendimiento sin igual y un coste total de propiedad considerablemente inferior. Los particulares planes de datos y gestión conforman una potente protección de los datos en la arquitectura del sistema.

Las funciones defensivas de InfiniBox le permiten proteger mejor los datos con snapshots/snapshots inmutables, replicación, cifrado y controles de gestión del acceso. Además, detectan amenazas más rápidamente gracias a alertas de umbrales de capacidad del grupo de almacenamiento y a una rápida recuperación con snapshots locales y replicadas.

InfiniSafe: Arquitectura de referencia para la gama InfiniBox

Ahora más que nunca resulta necesario saber cómo crear un entorno ciberresiliente para su almacenamiento primario. Las empresas necesitan una estrategia de varios niveles para seguir protegiendo sus activos de datos más críticos. La arquitectura de referencia de InfiniSafe define unas metodologías que se pueden aplicar con facilidad para ayudar a mejorar la ciberresiliencia. Este enfoque está basado en cuatro pilares:

- **Snapshots inmutables**
- **Aislamiento lógico remoto**
- **Entorno forense cerrado**
- **Recovery casi instantáneo**

Es fundamental crear copias protegidas e inalterables de sus datos. Estas se pueden considerar lógicamente aisladas por sí mismas, pero es importante ampliarlas mediante una práctica recomendada de replicación a una segunda copia inmutable, tal y como sucede con la recuperación ante desastres (DR, por sus siglas en inglés). Posteriormente, deberá comprobar o validar sus datos en dicha copia. Disponer de un entorno cerrado (a veces denominado de confianza cero o zero trust) le permite separarse de la producción y solo se activa durante el tiempo necesario para validar lo que específicamente quiere asegurarse de que está limpio. Usted puede utilizar las herramientas y aplicaciones que mejor le convengan para validar o comprobar los datos. Por último, una vez validados esos puntos en el tiempo, tendrá la posibilidad de recuperar los datos en cuestión de segundos o minutos. Al aprovechar nuestras capacidades de la gama InfiniBox, podrá disfrutar de todo esto sin la necesidad de ser propietario o depender de un vendor o un conjunto de herramientas en particular.

Snapshots: la piedra angular de la protección de datos y de la continuidad de negocio

El mecanismo de snapshot de Infinidat, InfiniSnap®, amplía las funciones críticas de protección de datos sin afectar a la escalabilidad o al rendimiento. InfiniSnap utiliza un mecanismo sin bloqueo redirigido a la escritura que crea snapshots y snapshots inmutables, y permite una rápida restauración bajo demanda.

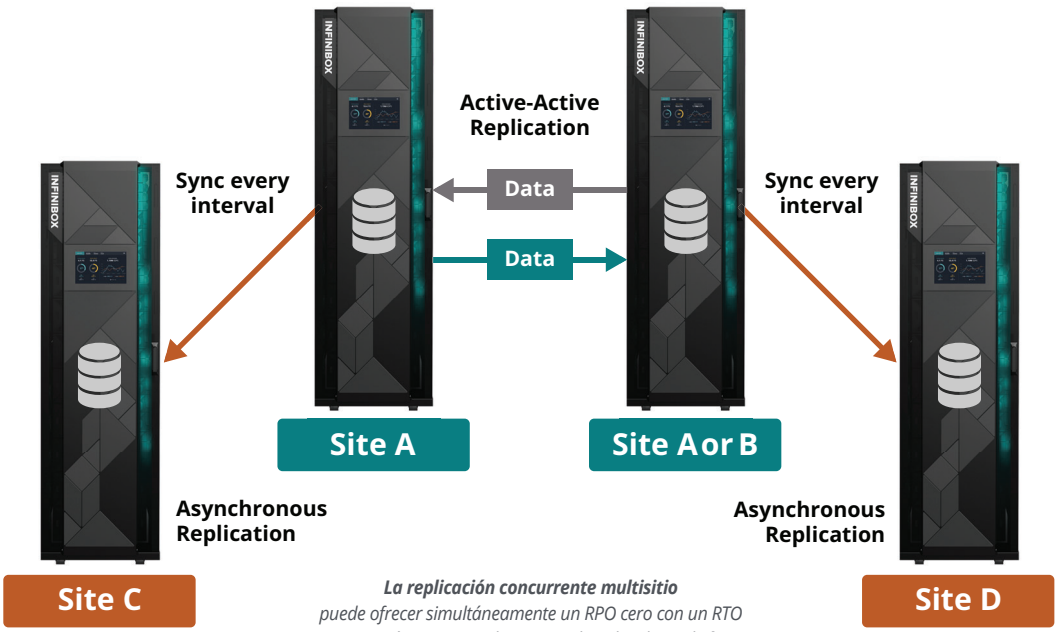
Las snapshots pueden ser de solo lectura o de escritura, y cada conjunto de datos puede almacenar hasta 1000 snapshots. Las snapshots de InfiniSnap habilitan snapshots inmutables para volúmenes, sistemas de archivos y grupos de consistencia. La función del directorio de snapshots permite a los usuarios finales examinar, seleccionar y recuperar fácilmente archivos que se han eliminado o modificado accidentalmente.

- **Snapshots inmutables:** las snapshots inmutables no pueden modificarse ni eliminarse dentro del período de retención establecido. Aunque los administradores pueden ampliar la fecha de vencimiento del bloqueo, no pueden acortarla. Si detectan un ataque, los administradores pueden acceder rápidamente a los datos y probarlos y hacer una recuperación utilizando el último snapshot anterior al ataque.
- **Detección de amenazas:** el cifrado del ransomware aumenta el tamaño de los datos, lo que incrementa el tamaño de las snapshots de los datos. Los administradores pueden establecer los umbrales de consumo de capacidad para ser advertidos si el volumen de las snapshots excede de repente los parámetros medios. Si detectan un ataque, los administradores pueden acceder rápidamente a los datos y probarlos, y hacer una recuperación utilizando la última snapshot anterior al ataque.

Replicación: potencie la continuidad de negocio

La replicación amplía el poder de las snapshots para proteger y recuperar datos amenazados. InfiniBox ofrece varios tipos de replicación para modificar necesidades ambientales.

- **Replicación asíncrona:** activa un objetivo del punto de recuperación (RPO) de 4 segundos. Al utilizar una infraestructura de IP, se reducen el coste y la complejidad.
- **Replicación síncrona:** activa un RPO de cero segundos con una latencia inferior a 400 microsegundos para aplicaciones de vital importancia. Si la red WAN se retrasa o falla, la replicación síncrona de InfiniBox vuelve al modo asíncrono. Si se restaura la red WAN, el motor replicará automáticamente todos los datos que faltan y reanudará la replicación síncrona sin la disrupción de I/O.
- **Replicación activa-activa:** los sistemas de InfiniBox permiten leer y escribir de forma simultánea en grupos de consistencia en áreas metropolitanas. Los volúmenes son imágenes externas que aparecen como multirrutas al mismo volumen. La replicación síncrona siempre mantiene la consistencia de los volúmenes. No hay relación maestro-esclavo, y no hay idas y venidas adicionales para actualizar la escritura en ningún volumen. Si es necesario, puede haber un testigo externo ligero en un nodo independiente o en una máquina virtual basada en la nube.
- **Replicación concurrente multisitio:** InfiniBox puede replicar de forma simultánea grupos de consistencia desde los sitios de replicación principales a otro sitio en un área metropolitana. A partir de aquí, los usuarios pueden replicar de forma asíncrona en una tercera ubicación remota.



***La replicación concurrente multisitio** puede ofrecer simultáneamente un RPO cero con un RTO cero en un área metropolitana y replicar los datos de forma asíncrona a un tercer o cuarto sitio situado a distancia con un RPO casi cero.*

INFINIDAT

Cifrado: protección de datos cifrados

El ransomware puede volver a cifrar archivos cifrados, que es el motivo por el que los snapshots y la replicación son la primera línea de defensa. Sin embargo, cuanto más seguro sea su cifrado, más difícil será para los hackers volver a cifrarlos.

- **Validación de los Estándares federales de procesamiento de la información (FIPS) 140-2:** El Instituto Nacional de Estándares y Tecnología (NIST) concedió la validación FIPS 140-2 al módulo criptográfico de Infinidat. El estándar certifica el uso de InfiniBox en un conjunto definido de proyectos de TI del Gobierno de Estados Unidos y de sectores regulados.
- **Unidades de autocifrado (SED) estándar con cifrado AES-256:** InfiniBox emplea unidades de autocifrado (SED) estándar con cifrado AES-256 de conformidad con el FIPS 140-2, las claves de autenticación más potentes que admiten las unidades.
- **Funciones de derivación de claves (KDF):** Infinidat utiliza tecnología KDF aprobada por el Gobierno federal de Estados Unidos que genera claves únicas a nivel global por unidad. Nuestro gestor de claves conectable facilita la gestión externa de claves a través del protocolo de interoperabilidad de gestión de claves (KMIP).
- **Integración con terceros:** mantiene una profunda integración con cualquier producto de cifrado como, por ejemplo, Thales, VMware, Oracle TDE o Microsoft TDE, sin programación especializada ni un alto coste.

Gestión del acceso: prohibido el paso

Existen varias vías por las que los ciberdelincuentes pueden acceder a una red. La más valiosa son las credenciales del administrador. InfiniBox ya está configurado para evitar que los ciberatacantes lleguen tan lejos: todos los accesos pasan por la API, y la API evita cualquier modificación de las snapshots, incluso con las credenciales del administrador.

Además, con la gestión del acceso de InfiniBox, los atacantes no llegarán lejos, para empezar.

- **Control de acceso basado en roles (RBAC):** RBAC se ejecuta en el plano de control del sistema para proteger cuentas locales y grupos de dominios/LDAP. La asignación de roles de grupo permite a los usuarios disponer de un control total, de un control sobre un conjunto de capacidades limitadas o de permisos de solo lectura. Los usuarios pueden desactivar o bloquear cuentas locales para que solo puedan utilizarse cuando los técnicos de Infinidat lleven a cabo actividades de mantenimiento. La autenticación de la sesión protege aún más el acceso administrativo.
- **Autenticación de hosts:** iSCSI utiliza CHAP para autenticar los hosts en el plano de datos. CHAP requiere una autenticación de hosts de varios factores para evitar que un host acceda a los datos de otro host.
- **Integración de gestión del acceso de terceros:** Infinidat se integra con soluciones de gestión del acceso externas, privilegiadas y de calidad empresarial, como CyberArk.
- **Acceso de estaciones de gestión y auditorías:** La gestión del acceso también incluye el acceso de estaciones de gestión a través de un enlace seguro, mientras que la auditoría sigue el registro de todas las operaciones que modifican los componentes o la configuración/estado de una máquina. Las auditorías también registran los cambios realizados por el administrador en la configuración.

CONCLUSIÓN

La protección de sus datos resulta crucial para el éxito de su negocio. El amplio conjunto de funciones empresariales de InfiniBox le permite desarrollar una ciberresiliencia y disponibilidad exhaustiva de sus datos, lo que convierte el almacenamiento en una parte de su estrategia de ciberseguridad corporativa general.

Cuando invierte en InfiniBox, no solo obtiene un rendimiento de calidad superior, un 100 % de disponibilidad, una facilidad de uso de tipo «instalar y olvidarse» y un coste total de propiedad notablemente inferior a gran escala, sino que también frustra los intentos de los posibles atacantes de ransomware. Los ciberdelincuentes se lucran a costa de víctimas que no están preparadas. No esperan toparse con potentes defensas de protección de los datos.

Evite estos ataques con las snapshots inmutables, la potente replicación, el sofisticado cifrado y la segura gestión del acceso de InfiniBox utilizando para ello un modelo todo incluido y adaptado a su presupuesto de almacenamiento, a sus empleados y a sus objetivos empresariales.