COHESITY

e-Book

Defienda sus datos frente a un ataque de ransomware

3 formas en las que Cohesity Next-Gen Data Management mejora la ciberresiliencia

La gran pregunta

El ransomware es el tipo de ciberdelito que crece con mayor rapidez. Los analistas predicen **que el ransomware atacará un negocio cada dos segundos** hacia finales de 2031.[1] Y cada vez que un ciberdelincuente se sale con la suya, la organización atacada resulta perjudicada tanto financieramente como en su reputación.

Se prevé que para 2025 se habrán creado, capturado, copiado y consumido más de 180 zettabytes de datos mundiales, según Statista.[2] En vista de que los datos crecen a un ritmo sin precedentes, ¿cómo podrá su producto de copias de seguridad y gestión de datos heredado estar a la altura?

Se supone que su copia de seguridad ayuda a proteger sus datos frente al ransomware, pero es probable que sus capacidades sean muy inferiores a las de la solución de gestión de datos de nueva generación de Cohesity. Su producto en sí puede constituir un blanco primario del ataque, ya que el 85 % de los sistemas destinatarios del ransomware son Windows.[3] Es posible que haga copias de seguridad de sus datos, pero estas no son inmunes a ataques sofisticados de ransomware. Además, si no dispone de detección temprana de anomalías con ayuda de inteligencia artificial/aprendizaje automático (IA/ML), seguramente no pueda detectar el ransomware proactivamente y recuperarse rápidamente, algo que Cohesity sí puede hacer.

¿Acaso su organización no se merece algo mejor? ¿Qué haría si supiera que ya existe una solución integral de copias de seguridad y gestión de datos creada específicamente para proteger, detectar y recuperarse rápidamente frente al ransomware? ¿No querría transformar, simplificar, salvaguardar y reforzar la protección de sus datos?

265 000

MILLONES USD

Coste previsto de los daños que causará el ransomware en todo el mundo en 2031.[4]

[1,4] Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031", 3 de junio de 2021.
[2] Statista. "Volume of Data Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025", 23 de mayo de 2022.
[3] SafetyDetectives. "Ransomware Facts, Trends, & Statistics for 2022".

Es solo cuestión de tiempo

A pesar del enorme esfuerzo invertido en poner freno a los ataques de ransomware, los ciberdelincuentes son innovadores y siguen creando nuevos programas maliciosos o "malware". Esto significa que los ataques de ransomware son cada vez más sofisticados y específicos, todo con el mismo objetivo: paralizar las operaciones comerciales con la esperanza de que las víctimas paguen para restaurar el orden.

Ningún sector está a salvo. Y debido a que las empresas son hoy en día blancos más atractivos que los consumidores, su organización debe prepararse proactivamente teniendo la certeza de que los ciberdelincuentes vendrán a por sus datos.

Protocolo TLP de los 10 malwares más importantes: WHITE

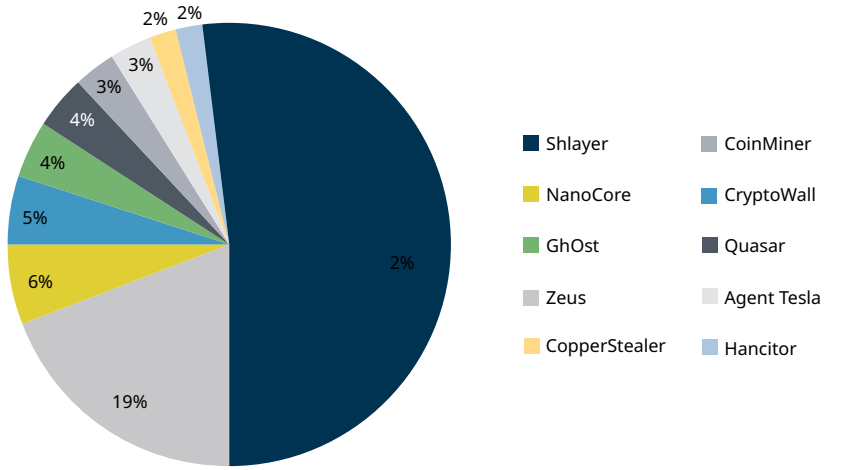


Figura 1. Desglose de los 10 malwares más importantes. Fuente: Center for Internet Security, mayo de 2021

Ahora van a por su mayor activo: sus datos

En la moderna economía digital, el éxito supone maximizar el uso de los datos de su organización para disfrutar de una ventaja competitiva. Pruebas de desarrollo, extracción de información y análisis son solo algunas de las formas en las que sus datos pueden trabajar para usted, y en especial los datos de sus copias de seguridad y otros datos no estructurados, que representan el 80 % de todos los datos empresariales.

Sin embargo, el crecimiento explosivo y el valor de esos datos es lo que los hace atractivos a los hackers que se ocultan tras el ransomware. Estos ciberdelincuentes han comenzado a atacar más agresivamente a sus copias de seguridad para hacerse con el control total de lo que desde hace mucho se considera la póliza de seguro de la continuidad del negocio.

79%

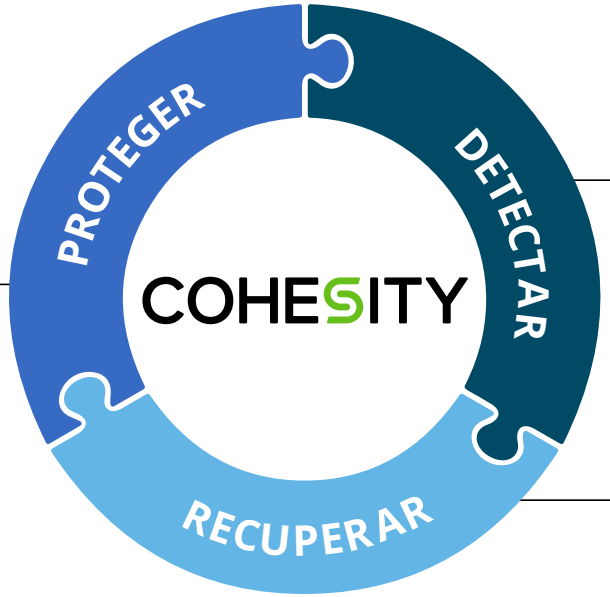
Organizaciones encuestadas que informan haber experimentado un ataque de ransomware durante el último año.[5]

[5] Enterprise Strategy Group. "The Long Road Ahead to Ransomware Preparedness", marzo de 2022.

3 claves para defender los datos de su copia de seguridad

El ritmo vertiginoso con el que cambia el modo y el lugar donde el malware hace acto de presencia hoy en día hace que resulte imposible para la empresa combatir cada posible nuevo ataque. Cohesity es una solución integral de gestión de datos de nueva generación creada para defender los datos de su copia de seguridad frente al ransomware.

- Copia de seguridad inmutable
- WORM (DataLock)
- RBAC
- MFA
- Marco de encriptación
- Quórum



- Detección temprana de anomalías con IA/ML
- Tasa de cambio diaria de los datos lógicos
- Tasa de cambio diaria de los datos almacenados
- Patrón basado en la captura de datos históricos

- Recomendación basada en aprendizaje automático
- Descubra vulnerabilidades para una recuperación limpia
- Restaure a escala
- Aislamiento de los datos

Adoptar un enfoque en múltiples capas de la protección de datos es el mejor modo de proteger los datos de su copia de seguridad frente a los ataques de ransomware. Este consiste en tres importantes conceptos que Cohesity integra:

Proteger	Detectar	Recuperar
Reduzca la superficie vulnerable al ataque y evite que sus copias de seguridad se conviertan en blanco de un ataque de ransomware con instantáneas inmutables de sus copias de seguridad, WORM y más capacidades de protección.	Utilice el aprendizaje automático para descubrir ataques de ransomware visibilizando las anomalías al monitorizar los datos durante la captura en el proceso de copia de seguridad.	Obtenga visibilidad profunda y cerciórese de que la recuperación de datos es limpia antes de restaurar al instante y de forma masiva todos sus datos en distintas ubicaciones y entornos.

1. Evite que su copia de seguridad sea blanco del ransomware

Las copias de seguridad son blanco del malware, que infecta la misma infraestructura que usted consideraba su mejor póliza de seguro. Una infraestructura de copias de seguridad vulnerada se convierte en una herramienta de los ciberdelincuentes, que además tienen el tiempo de su parte: por término medio, las organizaciones tardan 212 días en detectar una fuga de datos.[6] Y los encuestados creen que el trabajo remoto prolonga este tiempo.[7] El éxito de los ataques de ransomware suele tener consecuencias devastadoras: el coste medio de una fuga de datos es de 4,24 millones USD —9,23 millones USD en sanidad—, de los cuales la pérdida de productividad de TI y de los usuarios finales, el tiempo de inactividad y el robo de activos de información representan casi el 80 % de las repercusiones económicas.[8]
La plataforma de datos de nueva generación de Cohesity evita que sus copias de seguridad se conviertan en blanco de un ataque con mayor eficacia que Veritas:

- **Reduciendo su superficie vulnerable al ataque** – La arquitectura de muchos entornos está compuesta por productos puntuales fragmentados. Por el contrario, Cohesity consolida todos los componentes de copia de seguridad y recuperación de desastres en una sola plataforma global. Aparte de eso, Cohesity incluye deduplicación global de longitud variable en todas las fuentes de datos y compresión para reducir aún más las superficies vulnerables a ataques.
- **Fortaleciendo sus defensas con arquitectura de hiperescala** – Creados antes de la popularización de los entornos cloud, los entornos heredados carecen de capacidades de defensa frente a los ciberdelincuentes modernos:
  - **Instantáneas de estado inmutables de solo lectura** – La plataforma de Cohesity ha sido creada exprofeso para derrotar a los ciberatacantes. Cohesity protege las instantáneas de copia de seguridad y guarda estos datos en un estado inmutable. Dicha instantánea nunca es accesible ni se monta en aplicaciones externas. Las aplicaciones externas solo pueden acceder a los datos de la copia de seguridad en Cohesity mediante un clon de coste cero de la instantánea original en modo de lectura-escritura. Debido a este diseño exclusivo, el ransomware no puede modificar ni eliminar la instantánea inmutable de la copia de seguridad.
  - **Políticas DataLock** – Las capacidades de escritura única y lectura múltiple ("write-once-read-many", WORM) de Cohesity para realizar copias de seguridad permiten que determinados roles establezcan políticas DataLock inalterables para tareas seleccionadas. Por ejemplo, un responsable de seguridad puede almacenar copias de seguridad en formato WORM con un límite de tiempo para imponer una protección de datos que no pueda ser eliminada ni siquiera por un administrador o por ese mismo responsable de seguridad.
  - **Autenticación multifactorial (MFA)** – Toda persona que acceda a una copia de seguridad de Cohesity debe autenticarse empleando dos métodos de verificación.
  - **Encriptación de los datos** – Cohesity ofrece encriptación basada en software conforme al estándar FIPS y con arreglo a la norma AES-256 para datos en tránsito y en reposo. Se trata del módulo criptográfico validado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) según la norma Federal Information Processing Standards (FIPS) 140-2 de Nivel 1.
  - **Control de acceso basado en roles** – Cohesity reduce el riesgo de acceso no autorizado al permitir que el personal de TI conceda a cada persona el nivel mínimo de acceso a los datos que necesita para realizar una tarea concreta.
  - **Quórum** – Con Cohesity, todo cambio a nivel de raíz o de un sistema crítico debe ser autorizado por más de una persona para proteger los datos frente a amenazas internas y credenciales robadas.

[6-8] Ponemon Institute e IBM. "2021 Cost of Data Breach Report," Junio de 2021

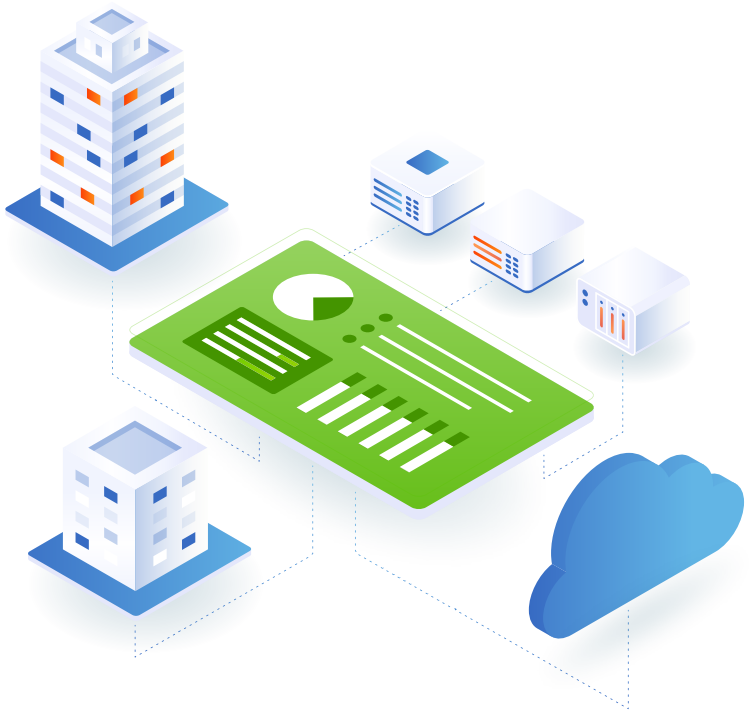
2. Detecte los ataques de ransomware

Los ataques de ransomware evolucionan con rapidez y buscan explotar sus datos y aplicaciones, ya residan estos en sus instalaciones o en un cloud público. Aunque los productos heredados carecen de capacidades para ayudarle a detectar los ataques, las funciones de detección de Cohesity mantienen a su equipo un paso por delante.

Tan solo Cohesity cuenta con una sola interfaz global basada en software como servicio (SaaS) y un panel de seguridad con los que su equipo podrá automatizar la monitorización, detectar cambios al momento y actuar con celeridad sobre sus datos y aplicaciones, con independencia de que residan en entornos autogestionados o gestionados por Cohesity:

- **Monitorización automática** – En la lucha contra el ransomware, el aprendizaje automático de Cohesity supone toda una ventaja. Cohesity ofrece información que una persona pasaría fácilmente por alto al monitorizar de forma continua y automática los datos capturados en fuentes primarias.
- **Reconozca patrones y cambios** – El algoritmo de aprendizaje automático de Cohesity establece patrones y busca automáticamente anomalías en la captura o tasa de cambio de los datos para detectar un posible ataque de ransomware en el entorno de producción de TI. Si la tasa de cambio de los datos de sus archivos primarios no concuerda con el rango del patrón normal —según las tasas de cambio diarias de los datos lógicos, los datos almacenados después de la deduplicación global o la captura de datos históricos—, la detección de anomalías de Cohesity acelera la reparación enviando una notificación a sus administradores de TI, así como al equipo de soporte de Cohesity.
- **Actúe rápidamente** – Una vez notificados, sus administradores de TI y el equipo de soporte de Cohesity pueden trabajar juntos para determinar los próximos pasos.

Además de monitorizar las tasas de cambio de los datos de las copias de seguridad para detectar posibles ataques de ransomware, Cohesity detecta y advierte de anomalías a nivel de archivo dentro de los archivos no estructurados y datos de objetos. Por ejemplo, con Cohesity Spotlight —una aplicación de Cohesity Marketplace que se ejecuta directamente en la plataforma Cohesity—, su equipo puede buscar fácilmente registros de auditorías para hallar patrones anómalos de acceso a los archivos. Esto incluye analizar la frecuencia de los archivos a los que se ha accedido, el número de archivos que está siendo modificado, los archivos añadidos o eliminados por un usuario o una aplicación específicos, etc. Estas capacidades pueden ayudar a detectar con rapidez un ataque de ransomware.



3. Recupérese con rapidez sin pagar un rescate

En caso de que suceda lo peor y los atacantes exijan un rescate, debe asegurarse de que su negocio y sus usuarios disfrutan de la recuperación más rápida posible, a escala.

Cohesity tiene capacidades de las que carecen otros productos para que su equipo vuelva enseguida al trabajo:

- **Aislamiento de los datos** – El personal de TI puede duplicar los datos automáticamente en otro clúster inmutable de Cohesity en las instalaciones o en el cloud público para garantizar que siempre haya disponible una copia inmutable adicional de los datos.
- **Visibilidad profunda para una recuperación limpia y de confianza** – Cohesity mitiga el riesgo evitando que se reintroduzca una cibervulnerabilidad en el entorno de producción durante la restauración de los datos. Un panel de control detallado muestra a su equipo el estado de salud y el índice de cibervulnerabilidad de la instantánea de su copia de seguridad. Solo tiene que recuperarla a un momento en el tiempo en el que estaba limpia para cumplir los acuerdos de nivel de servicio (SLA) de su negocio.
- **Escalabilidad sin límites** – Debido a que Cohesity está diseñada sobre una arquitectura de hiperescala, permite que los administradores de TI amplíen sus clústers de Cohesity de forma ilimitada y almacenar instantáneas y clones sin límite y sin efecto sobre el rendimiento. Y sus datos siempre estarán cerca, lo que acelera la recuperación, puesto que no es necesario reintroducir los datos desde una ubicación externa.
- **Búsqueda global procesable** – Con la función exclusiva de búsqueda global de Cohesity, usted y sus equipos podrán localizar rápidamente datos y archivos infectados específicos y tomar las medidas correctivas adecuadas. Algunas de estas medidas consisten en encontrar un archivo malicioso en todas las cargas de trabajo y llevar a cabo las acciones necesarias para contenerlo. La búsqueda de Cohesity también puede recomendar el momento en el tiempo más limpio para la recuperación.
- **Restauración masiva al instante** – El ransomware rara vez se limita a atacar una o dos máquinas virtuales (MV) o archivos, sino que se trata de una situación de recuperación tras un desastre que requiere una solución avanzada y moderna capaz de recuperar al instante cientos de MV, incluidas las de estado puro o "bare metal", a escala y a cualquier momento en el tiempo. Al contrario que otras soluciones, que pueden tardar días, o incluso semanas, en recuperar un gran número de MV, la restauración masiva instantánea de Cohesity ha demostrado una eficacia insuperable.

"Nuestra organización sufrió un grave ataque de ransomware que inutilizó toda nuestra infraestructura. Con Cohesity fuimos capaces de recuperar máquinas y archivos compartidos, verificar que estaban limpios y volver a poner en funcionamiento las aplicaciones.
Cohesity nos ha ahorrado literalmente cientos de horas de trabajo, y hasta diría que nos ha librado de tener que pagar la petición de rescate. Conservamos nuestros trabajos y la comunidad dispone de un hospital funcional porque hemos obtenido excelentes resultados con Cohesity".

– Sam Stewart, analista de sistemas de red de Sky Lakes

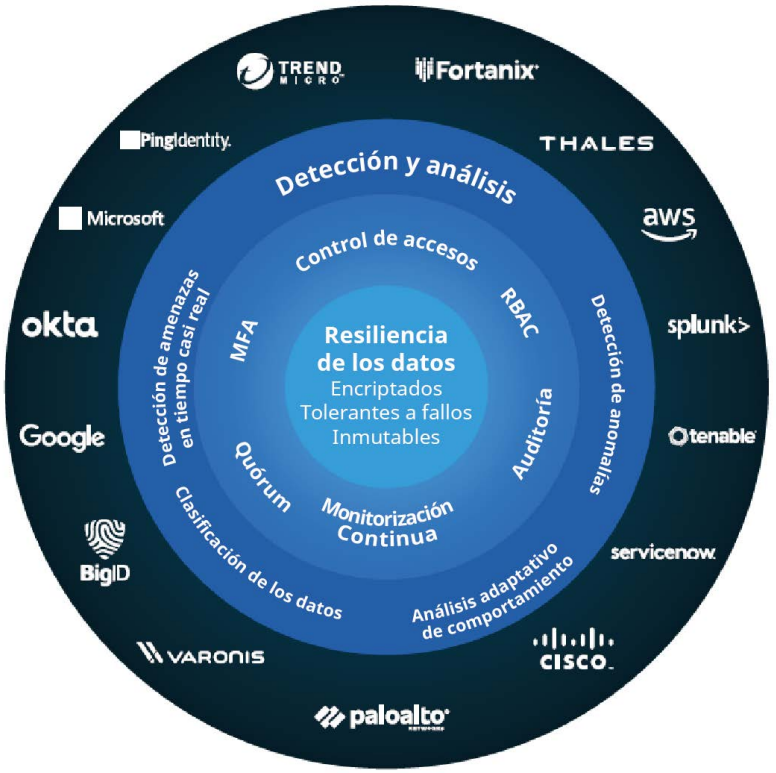
Sky Lakes Medical

Mejore su ciberresiliencia con Cohesity Threat Defense

Además de potenciar sus copias de seguridad, la arquitectura Cohesity Threat Defense le ayuda a mantener sus datos a buen recaudo como parte de una arquitectura global de seguridad y una estrategia de defensa en profundidad.

- Derrote a los atacantes mediante controles de acceso avanzado.
- Detecte amenazas de forma inmediata identificando anomalías y ataques en tiempo real.
- Refuerce su postura de seguridad mediante la estrecha integración con soluciones de seguridad de terceros.

Con tecnología IA



Ciberresiliente

Descargue el informe técnico "Amplifique sus defensas frente al Ransomware: proteja, detecte y recupere" (solo disponible en inglés) para conocer más detalles técnicos.

Encontrará más información en www.cohesity.com/ransomware