RESUMEN DE LA SOLUCIÓN

Lenovo INFINIDAT

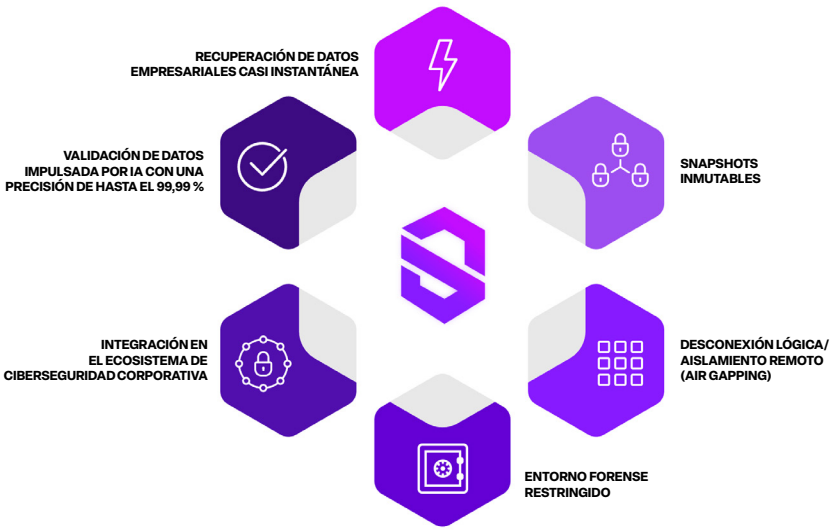
InfiniSafe® Cyber Detection

Se espera que el impacto de la ciberdelincuencia cueste a las empresas 9,5 billones USD al año.[1] Cada 39 segundos, se produce un nuevo ataque en la red.[2] Los costes para una empresa incluyen daños y destrucción de datos, pérdida de productividad, robo de la propiedad intelectual, robo de datos personales y financieros, malversación, etc. A la disrupción del negocio tras el ataque, hay que sumar la investigación forense, la detección y la restauración de los datos y sistemas pirateados, así como la pérdida de confianza y reputación. La mayoría de los equipos de seguridad y TI considera que es solo cuestión de tiempo que sufran un ciberataque. ¿Está preparado?

Nuestra estrategia de protección y recuperación de datos de nueva generación da prioridad a la recuperación frente a los ciberataques. Los servicios de ciberresiliencia de nuestra plataforma InfiniVerse®, proporcionados por InfiniSafe, respaldan directamente las amplias capacidades de ciberalmacenamiento, lo que le ofrece una protección, prevención, detección y capacidad de recuperación garantizada de extremo a extremo. El diseño seguro de InfiniSafe consta de la pila cibernética central, InfiniSafe Automated Cyber Protection (ACP) e InfiniSafe Cyber Detection.

InfiniSafe Cyber Detection mejora las capacidades centrales de resiliencia y respuesta de la pila cibernética de Infinidat al permitir a los equipos de seguridad y TI detectar ataques de ransomware y malware con una precisión de hasta el 99,99 %, además de hacer posible la recuperación casi instantánea de los datos a partir de copias limpias «en buen estado» en las plataformas InfiniBox® e InfiniBox™ SSA. Esto le devuelve la ventaja sobre los atacantes.

InfiniSafe Cyber Detection añade un nivel de detección de datos a la pila cibernética de InfiniSafe que envuelve las cuatro capas principales de la pila y aumenta la capacidad de InfiniSafe para detectar ciberincidentes. InfiniSafe Cyber Detection explora en profundidad los almacenes de bloques, archivos, bases de datos y almacenes de datos VMware presentando snapshots inmutables de InfiniBox e InfiniBox SSA a potentes motores de análisis basados en inteligencia artificial que validan su integridad y, mediante el aprendizaje automático, identifican cualquier cambio malicioso que pudiera indicar un ciberataque.



InfiniSafe ACP se integra directamente en sus operaciones de seguridad. Cuando se detecta un ataque, ejecuta automáticamente snapshots inmutables y los presenta a InfiniSafe Cyber Detection, que los escanea en profundidad y proporciona amplios informes forenses para diagnosticar qué datos se han visto vulnerados y la naturaleza de dicha vulneración. Esto proporciona información esencial sobre el origen de los datos comprometidos. A continuación, gracias a la potencia de la tecnología InfiniSafe, el usuario puede recuperar rápidamente el funcionamiento normal de la empresa una vez que ha identificado una copia de los datos en buen estado.

El 65 % de los profesionales de TI y ciberseguridad encuestados consideran el ransomware entre las 3 principales amenazas para su organización

Informe ESG: Preparación frente al ransomware en 2023

Detección

Análisis y detección mediante aprendizaje automático

Análisis forense

Informes forenses para diagnosticar e identificar el impacto del ataque

Recuperación

Informes sobre la última versión en buen estado de los archivos para agilizar la recuperación

InfiniSafe Cyber Detection se entrena continuamente con una combinación de más de 200 análisis basados en la inspección del contenido completo de los archivos y de los datos, no solo los metadatos. Gracias a los potentes algoritmos de aprendizaje automático, no necesitamos conocer todas las nuevas variantes que puedan surgir. La profundidad de nuestro escaneo determina tanto las variantes conocidas como las desconocidas, así como los cifrados parciales. Siempre sabrá si algo es sospechoso y, en el caso de una variante conocida, le indicaremos el tipo específico de variante que se utilizó para corromper o identificar los resultados, incluso sin nombres específicos de variantes, con una precisión del 99,99 %. Esto ayuda a las empresas a proteger su infraestructura y su contenido críticos para el negocio sin recibir falsos positivos para que pueda centrarse en las áreas que son realmente motivo de preocupación y resolver los problemas rápidamente. Si a esto le añadimos nuestra amplia automatización y orquestación, además de la integración de seguridad con InfiniSafe ACP, dispone de una de las soluciones de resiliencia de ciberalmacenamiento de extremo a extremo más completas del mercado.

Detección

Safe Cyber Detection utiliza análisis del contenido completo en todos los datos protegidos. Este profundo conocimiento es la única manera de confiar en la integridad de sus datos y de tener la certeza de que los ciberdelincuentes no están burlando sus herramientas de análisis de datos, ocultando su rastro y dañando sus datos de manera encubierta.

Al igual que ocurre con la caché neuronal de aprendizaje automático de nuestra plataforma InfiniBox, InfiniSafe Cyber Detection se ha enriquecido con un "machine learning" potente y determinista. Combina más de 200 análisis —-que superan en 20 veces a los de la competencia— con observaciones de datos que se vuelven más inteligentes con el tiempo a medida que se agregan más observaciones. El aprendizaje automático se entrena con miles de infecciones de ransomware, malware y troyanos para encontrar patrones de comportamiento poco habituales y distinguir la actividad del usuario del ransomware, minimizando al mismo tiempo los falsos positivos y negativos.

Análisis forense

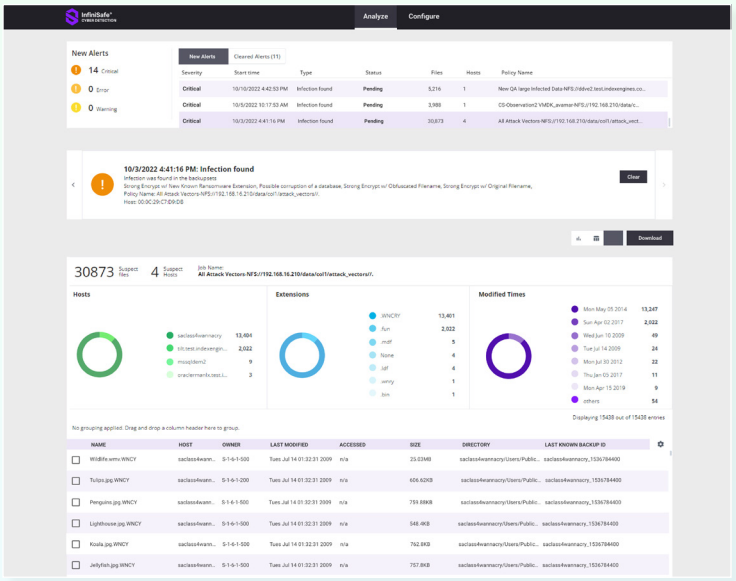
Cuando los datos están dañados, InfiniSafe Cyber Detection genera una lista de los archivos dañados. Los archivos dañados se etiquetan, y se crean informes forenses para diagnosticar e identificar el impacto del ataque y proporcionar la inteligencia necesaria para facilitar la recuperación.

Alertas organizadas por gravedad

Nuevos datos sobre sospechas de daños

Gráficos personalizables y dinámicos para profundizar en los detalles del ataque

Lista de archivos dañados que se puede descargar

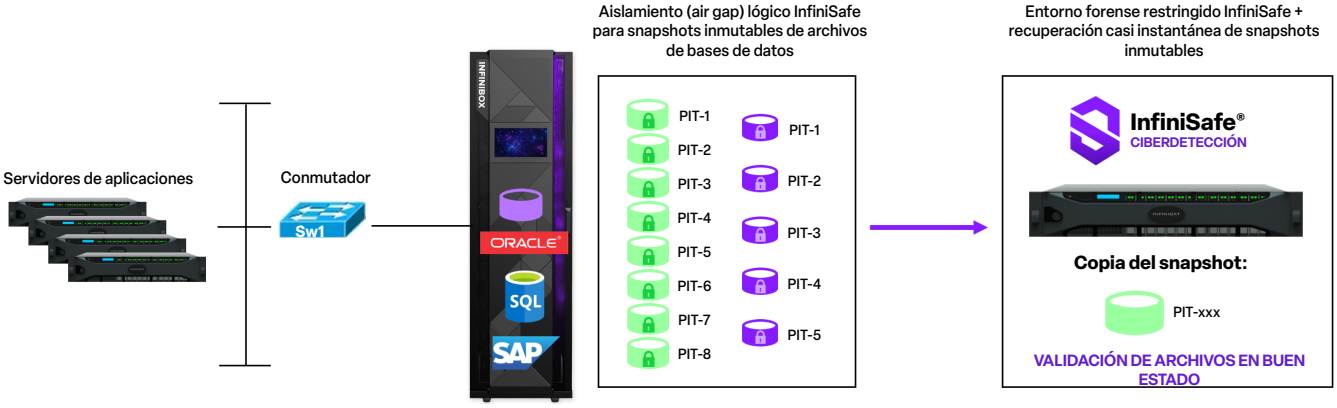


Panel de control posterior al ataque: mejor experiencia del usuario, mayor información sobre los datos y flujo de trabajo intuitivo posterior al ataque.

Recuperación

Por último, InfiniSafe Cyber Detection informa sobre la última copia en buen estado de un archivo o de una copia de seguridad cuando esta última se ubique en una plataforma InfiniBox o InfiniBox SSA. Sabe dónde se encuentran los datos dañados, dónde está la última versión en buen estado de los datos y en qué snapshots o conjuntos de copias de seguridad estaban los datos para agilizar el proceso de recuperación.

Casos prácticos: ciberdetección de bloques, archivos y bases de datos



Las empresas que utilizan InfiniBox o InfiniBox SSA para aplicaciones de bases de datos críticas para la organización pueden estar seguras de que, al utilizar la tecnología de pila cibernética InfiniSafe con Cyber Detection, pueden tomar snapshots inmutables frecuentes para validar su integridad y, mediante el aprendizaje automático, identificar cualquier cambio que indique un ciberataque. InfiniSafe Cyber Detection determina cualquier problema e informa sobre copias de datos en buen estado para su recuperación casi instantánea con InfiniSafe.

Cyber Detection Array

Las empresas que utilizan varias plataformas InfiniBox o InfiniBox SSA pueden replicar los datos en una matriz de ciberdetección designada, Cyber Detection Array, en un entorno forense restringido utilizando las herramientas de replicación nativas de Infinidat. Cyber Detection Array analiza todos los archivos de datos, etiqueta los archivos dañados y crea un informe forense. Esta configuración proporciona a las empresas la inteligencia necesaria para detectar un ciberataque.

El ransomware malicioso y los incidentes de malware siguen afectando a empresas y servicios críticos, desde infraestructuras de energía hasta escuelas y hospitales. Las pérdidas económicas totales derivadas de los ataques de ransomware y malware siguen aumentando. La aplicación de una estrategia eficaz de protección y recuperación de datos de próxima generación puede mitigar la exposición de su empresa y garantizar una rápida recuperación.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

iberia@infinidat.com

 | © 2026 Infinidat, una società del gruppo Lenovo

Lenovo INFINIDAT