InfiniSafe® Cyber Detection

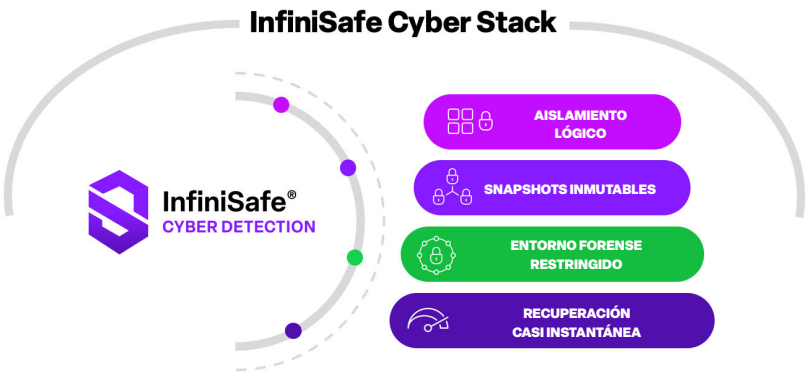
Se espera que el impacto de la ciberdelincuencia cueste a las empresas 8 billones USD al año.[1] Cada 39 segundos, se produce un nuevo ataque en algún lugar de la red.[2] Los costes para una empresa incluyen daños y destrucción de datos, pérdida de productividad, robo de la propiedad intelectual, robo 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 de los sistemas pirateados, y la pérdida de confianza y reputación. La mayoría de los equipos de seguridad y TI cree que es solo cuestión de tiempo que sufran un ciberataque. ¿Está preparado?

La tecnología InfiniSafe proporciona una pila cibernética de varias capas para la creación de entornos resilientes de ciberalmacenamiento con las plataformas InfiniBox® e InfiniBox™ SSA.

La introducción de InfiniSafe Cyber Detection mejora las capacidades de resiliencia y respuesta del ciberalmacenamiento de Infinidat al permitir a los equipos de seguridad y TI detectar ataques de ransomware y malware con una precisión de hasta el 99,5 %, 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.

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 y bases de datos presentando snapshots inmutables de InfiniBox e InfiniBox SSA a potentes motores de análisis basados en la inteligencia artificial que validarán su integridad y, mediante el aprendizaje automático, identificarán cualquier cambio malicioso que pudiera indicar un ciberataque.

Cuando se detecta un ataque, InfiniSafe Cyber Detection proporciona informes forenses para diagnosticar qué datos se han visto comprometidos y la naturaleza del incidente de seguridad, y ofrece información crítica 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.



InfiniSafe Cyber Detection utiliza 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. Los potentes algoritmos de aprendizaje automático le indicarán el tipo de variante que se ha utilizado para dañar los datos con una precisión del 99,5 %, lo que 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 se identifica un daño en los datos, InfiniSafe Cyber Detection proporciona las herramientas forenses necesarias para diagnosticar, identificar y ayudar a recuperar los activos afectados. InfiniSafe Cyber Detection informa sobre los archivos afectados, y los resultados forenses pueden ser investigados por sus equipos de seguridad y de software, por lo que cualquier problema puede erradicarse con sus herramientas, según sea necesario. De esta forma, cualquier dato comprometido puede sustituirse fácilmente por la última versión en buen estado para garantizar que la actividad de la empresa vuelva a la normalidad con un tiempo de inactividad mínimo.

> «El **79%** de las organizaciones afirma que la **preparación para el ransomware** es una de las cinco principales **prioridades empresariales** en general a ojos del equipo ejecutivo y/o del consejo de administración».
>
> Informe de investigación de Enterprise Strategy Group, The Long Road Ahead to Ransomware Prepareness (El largo camino por recorrer en la preparación para el ransomware), junio de 2022

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 es una opción complementaria a nuestra tecnología básica InfiniSafe y constituye una licencia basada en suscripción. InfiniSafe Cyber Detection es un producto posterior al ataque que se centra en la resiliencia de los datos en la pila cibernética de InfiniSafe y no sustituye a las prácticas recomendadas de prevención del ransomware y del malware ni a los productos tradicionales de gestión de amenazas en lo que a la parte de los servidores, de las aplicaciones y de las redes de la estrategia general de ciberseguridad se refiere.

Detección

InfiniSafe 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 nuestra caché neuronal de aprendizaje automático, InfiniSafe Cyber Detection se ha enriquecido con un aprendizaje automático potente y determinista, que 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

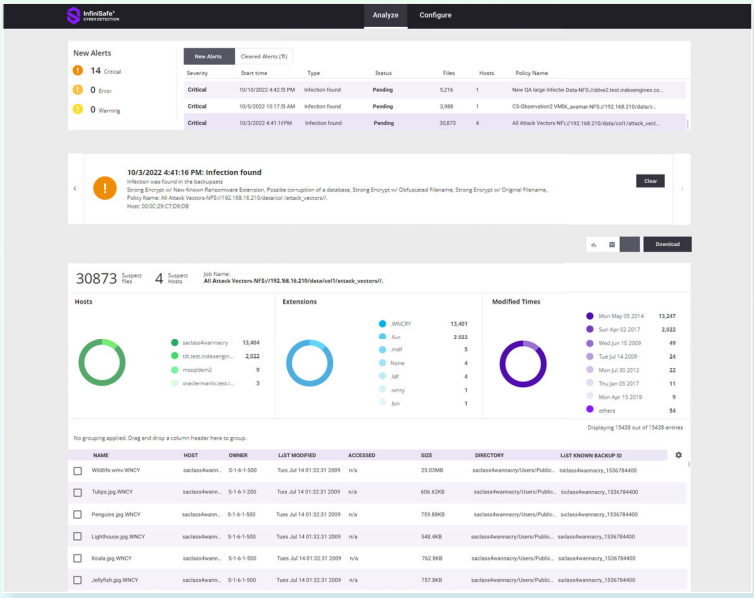
Cuando los datos están dañados, InfiniSafe Cyber Detection genera una lista de los archivos dañados. Los archivos dañados se etiquetan, y se crean informes forenses para diagnosticar e identificar el impacto del ataque y proporcionar la inteligencia necesaria para facilitar la recuperación.

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

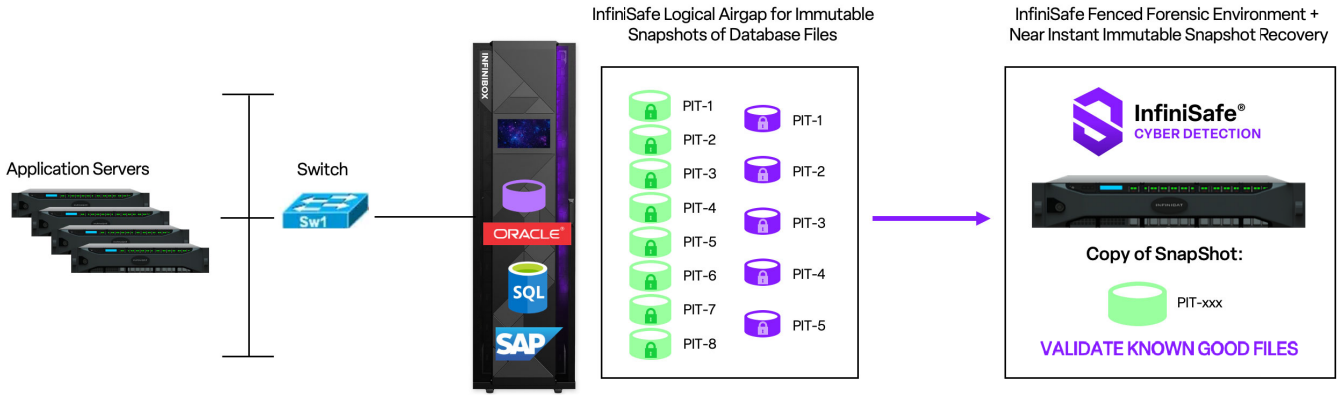


Panel de control posterior al ataque: mejor experiencia del usuario, mayor información sobre los datos y flujo de trabajo intuitivo posterior al ataque.

Recuperación

Por último, InfiniSafe Cyber Detection informará 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. Sabrá 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, a través del aprendizaje automático, identificar cualquier cambio que indique un ciberataque. InfiniSafe Cyber Detection determinará cualquier problema e informará 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 de malware siguen aumentando. La aplicación de una estrategia eficaz de ciberdetección puede mitigar la exposición de su empresa y garantizar una rápida recuperación.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

iberia@infinidat.com

INFINIDAT