RESUMEN DE LA SOLUCIÓN

Ciberprotección automatizada InfiniSafe®: reducir la amenaza

Lenovo INFINIDAT

Reducir la ventana de amenaza para evitar o tratar de prevenir los ciberataques es más importante que nunca. Ninguna solución puede abordar todas las vulnerabilidades, pero disponer de un conjunto muy flexible de capacidades y opciones para proteger los activos de datos críticos de una empresa es una pieza importante de un rompecabezas complejo. **Recuerde: no se trata de si los ciberatacantes atacarán, sino de cuándo lo harán.**

Prepárese

En la actualidad, la mayoría de las organizaciones protegen sus datos mediante métodos tradicionales de copia de seguridad y recuperación, como los snapshots eliminables. Si refuerza estos métodos con snapshots programados, inmutables y bloqueados por temporizador, habrá hecho un enorme progreso en la seguridad de sus datos. Por desgracia, los eventos programados crean grandes lagunas que hacen que los datos sean vulnerables. El intervalo de tiempo entre estos puntos suele estar determinado por el objetivo de punto de recuperación o RPO, una medida de la cantidad de datos que una empresa puede permitirse perder en un tiempo determinado. Si se realizan instantáneas inmutables cuatro veces al día, esto significa un RPO de hasta 6 horas. Hoy en día, la cantidad de datos que podrían verse comprometidos en ese tiempo puede suponer la ruina de una empresa.

Por lo tanto, es necesario un proceso más proactivo para proteger los datos en caso de que se sospeche de un ataque. Los equipos de supervisión de la seguridad no pueden reaccionar con la rapidez suficiente para proteger los datos durante ciberataques que se mueven a la velocidad de las redes y la computación. La ciberprotección automatizada de InfiniSafe hace frente a este problema. Aprovechando la supervisión en tiempo real que existe en los centros de operaciones de seguridad de muchas empresas y la velocidad de computación en cualquier nivel de alerta, un equipo de seguridad puede definir un activador para crear automática e inmediatamente snapshots inmutables en un entorno de almacenamiento Infinidat, reduciendo así el riesgo de corrupción de datos dañinos, borrado de datos, cifrado de datos, etc.

Todo ataque consiste en obtener información y ventaja. Cifrando datos, corrompiendo copias de seguridad y robando información se crea una ventaja. Cuando los atacantes tienen ventaja, saben que es probable que puedan extorsionarle de alguna manera.

El tiempo es dinero: mucho dinero cuando se trata de ciberincidentes. Las empresas se ven sumidas en el caos cuando se produce un ciberevento de tal magnitud. Cuanto más rápidamente se asegure de que dispone de sus datos y de que están en un estado bueno y conocido, antes recuperará parte

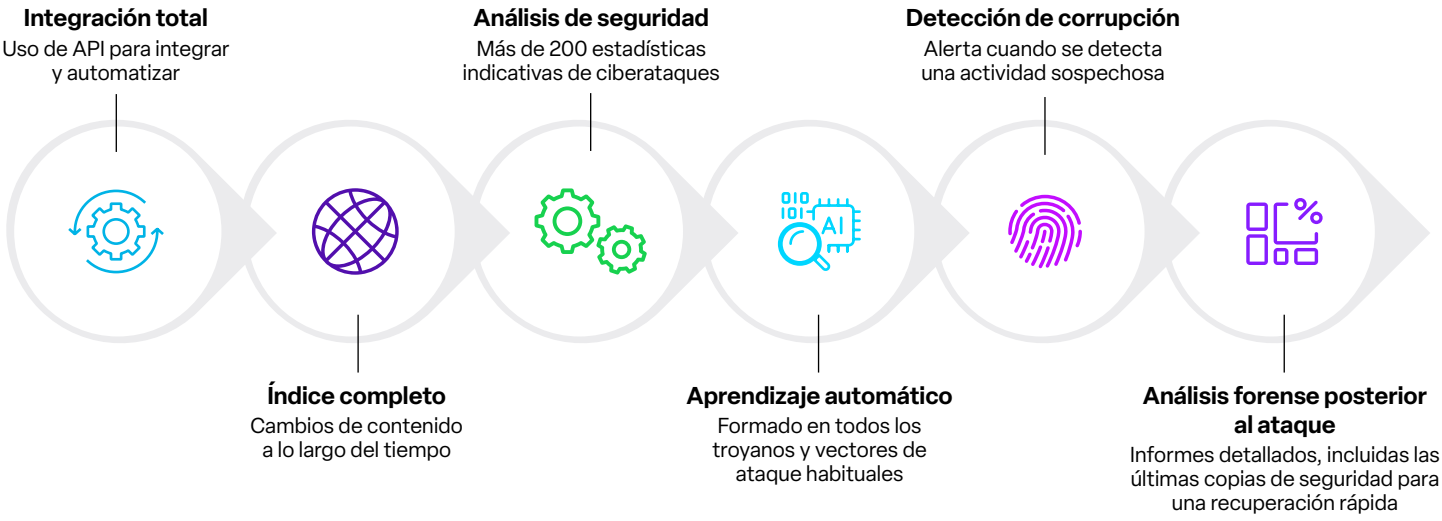
Pila cibernética InfiniSafe

de su ventaja, si no toda. Disponemos de todos los mecanismos a nuestro alrededor para ayudar a que los ciberdesastres sean más fáciles de afrontar; sin embargo, debemos juntar las piezas de estas soluciones y orquestar el proceso, pues los atacantes quieren crear el caos y no darle tiempo para pensar.

Identificar, orquestar y actuar

Hoy en día, las empresas cuentan con entornos complejos y multicapa que comprenden numerosas herramientas, sistemas de supervisión y procesos. En el centro de todo ello, muchos tienen Centros de Operaciones de Seguridad (SOC) específicos. Dentro del SOC, hay una serie de aplicaciones diseñadas para la seguridad de las infraestructuras, muchas de ellas etiquetadas como soluciones SIEM (Security Information and Event Management, o gestión de información y eventos de seguridad) y SOAR (Security Orchestration And Response, u orquestación y respuesta de seguridad). Los entornos SIEM y SOAR son el punto central de recogida de casi todo lo relacionado con la seguridad en cuanto se detecta un problema. El siguiente paso es crear un proceso bien definido y orquestado que se ejecute a la velocidad de computación sin necesidad de la lenta intervención humana. Las fracciones de segundo importan, y una ejecución casi instantánea es importante para tener una oportunidad de limitar la exposición.

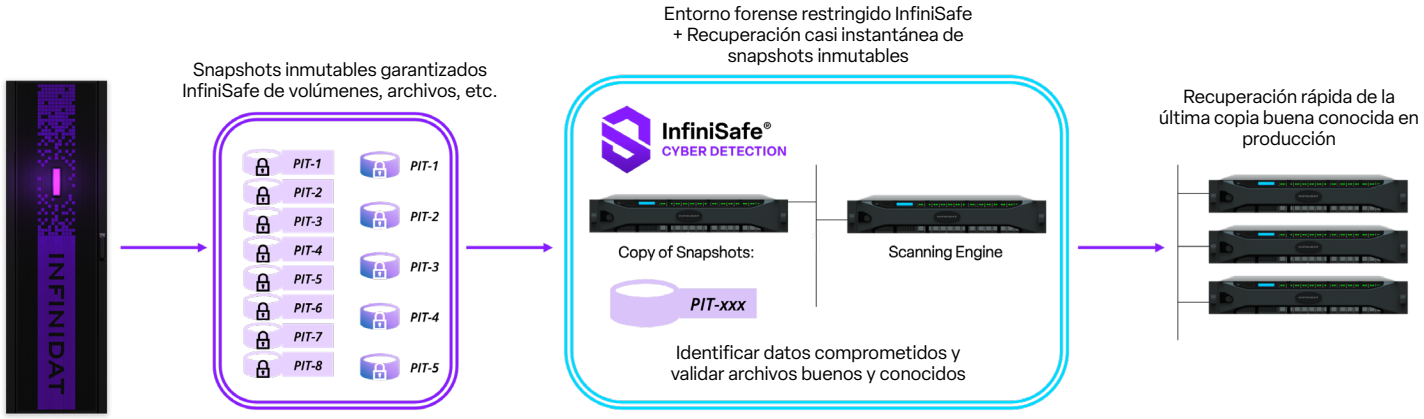
¿Cómo lo consigue Infinidat? Muy sencillo. Desde hace años, nuestros productos disponen de las capacidades InfiniSafe. Disponemos de una potente arquitectura de referencia de InfiniSafe para la familia InfiniBox que se amplía y orquesta fácilmente para ser activada por cualquier evento, en cualquier lugar. En este caso, se podría activar por los entornos SIEM o SOAR de una empresa. Estos entornos de aplicación disponen de interfaces ampliables, a través de API o CLI; su vinculación con la arquitectura de referencia InfiniSafe bien definida



proporciona un conjunto totalmente automatizado de capacidades que pueden orquestarse para crear de forma proactiva y rápida snapshots inmutables para proteger sus activos de datos primarios más críticos.

Validar los datos y recuperarlos rápidamente

InfiniSafe también tiene la capacidad de orquestar la creación de un entorno forense restringido, un espacio de red privado y limpio separado de una red o sistemas de usuarios internos posiblemente afectados. Usted puede y debe disponer de un conjunto de recursos fuera de producción para probar y validar sus datos con las herramientas y el software necesarios. A continuación, InfiniSafe puede presentar instantáneamente



snapshots inmutables de volúmenes o sistemas de archivos al entorno forense restringido, adjuntarlos y utilizar todas las herramientas a su disposición para validar sus datos. Infinidat también puede ayudar en ese proceso de validación, con herramientas potentes y esclarecedoras.

InfiniSafe Cyber Detection es una solución complementaria a los componentes de InfiniSafe que, por lo demás, no tienen coste alguno. InfiniSafe Cyber Detection analiza en profundidad los almacenes de bloques, archivos y bases de datos presentando snapshots inmutables de InfiniBox e InfiniBox™ SSA a un potente motor de análisis basado en IA. El análisis consiste en validar la integridad de los datos y, mediante el aprendizaje automático basado en IA, identificar cualquier cambio malicioso como resultado de un ciberataque. Y lo que es más importante, el análisis utiliza más de 200 puntos de datos para determinar qué datos pueden haberse visto comprometidos, con una precisión del 99,99 %. Este nivel de precisión y detalle hace que cualquier análisis forense adicional esté muy definido y sea fácil actuar sobre él, minimizando cualquier posible falso positivo, ya que es necesario actuar con rapidez y previsión ante un ciberevento. La ampliación de esta funcionalidad a InfiniSafe Cyber Detection requiere la adquisición de licencias de capacidad adecuadas para el análisis.

Resumen

«Los malos» crean el caos y se apoderan de sus activos de datos más importantes si no se está preparado. Conocer el estado de sus datos manteniéndolos protegidos de forma proactiva, más allá de simples eventos programados, es un componente clave para reducir la ventana de amenazas, recuperar la ventaja y frustrar a quienes buscan extorsionarle poniendo en peligro sus datos.

iberia@infinidat.com

Lenovo
INFINIDAT