SOLUTION BRIEF

InfiniSafe® Automated Cyber Protection: limitare la minaccia

Lenovo INFINIDAT

Oggi, ridurre la finestra di minaccia per evitare o cercare di prevenire gli attacchi informatici è più importante che mai. Nessuna soluzione è in grado di gestire ogni singola vulnerabilità, ma disporre di un insieme altamente flessibile di funzionalità e opzioni per proteggere le risorse di dati critiche di un'azienda è una tessera importante di un puzzle complesso. **Ricorda: la questione non è "se" gli aggressori informatici colpiranno, ma "quando".**

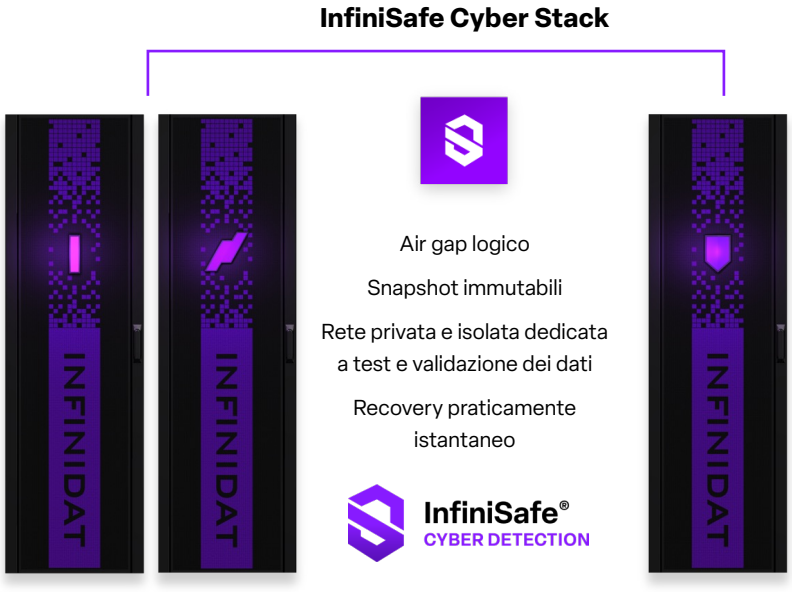
Prepararsi

Attualmente, la maggior parte delle organizzazioni protegge i dati utilizzando strumenti di backup e ripristino tradizionali, tra cui le snapshot eliminabili. Se a questi metodi si aggiungono snapshot immutabili programmate e bloccate da un timer, si aumenta in maniera incrementale la protezione dei dati. Purtroppo, però, gli eventi programmati creano ampie lacune che rendono i dati vulnerabili. Il gap temporale è in genere determinato dall'obiettivo del punto di ripristino o RPO , una misura della quantità di dati che un'azienda può permettersi di perdere in un determinato periodo di tempo. Se le snaphot immutabili vengono eseguite quattro volte al giorno, un RPO può arrivare fino a 6 ore. Oggi, la quantità di dati che potrebbe essere compromessa in questo lasso di tempo può rovinare un'azienda.

Di conseguenza, in caso di sospetto attacco, è necessario un processo più proattivo per proteggere i dati. I team di monitoraggio della sicurezza non sono in grado di reagire abbastanza velocemente per proteggere i dati durante eventi informatici che si muovono alla velocità delle reti e dell'elaborazione. InfiniSafe Automated Cyber Protection affronta questo problema. Sfruttando il monitoraggio in tempo reale che esiste all'interno di molti centri operativi di sicurezza aziendali e la velocità di elaborazione di qualsiasi livello di allarme, un team di sicurezza può definire un trigger per creare automaticamente e immediatamente snapshot immutabili in un ambiente di storage Infinidat, riducendo così il rischio di pericolosi danneggiamenti, cancellazione, crittografia dei dati, ecc.

Ogni attacco mira a ottenere informazioni e un vantaggio. La crittografia dei dati, la corruzione dei backup e il furto di informazioni creano questo vantaggio. Quando gli aggressori si trovano in questa situazione, sanno che probabilmente saranno in grado di estorcere un riscatto.

Il tempo è denaro, molto denaro quando si tratta di incidenti informatici. Le aziende vengono gettate nel caos quando si verifica un evento informatico di tale portata. La velocità con cui si riescono a ottenere dati di validità certa è fondamentale per recuperare il proprio vantaggio, in parte se non del tutto. Abbiamo a disposizione tutti i meccanismi

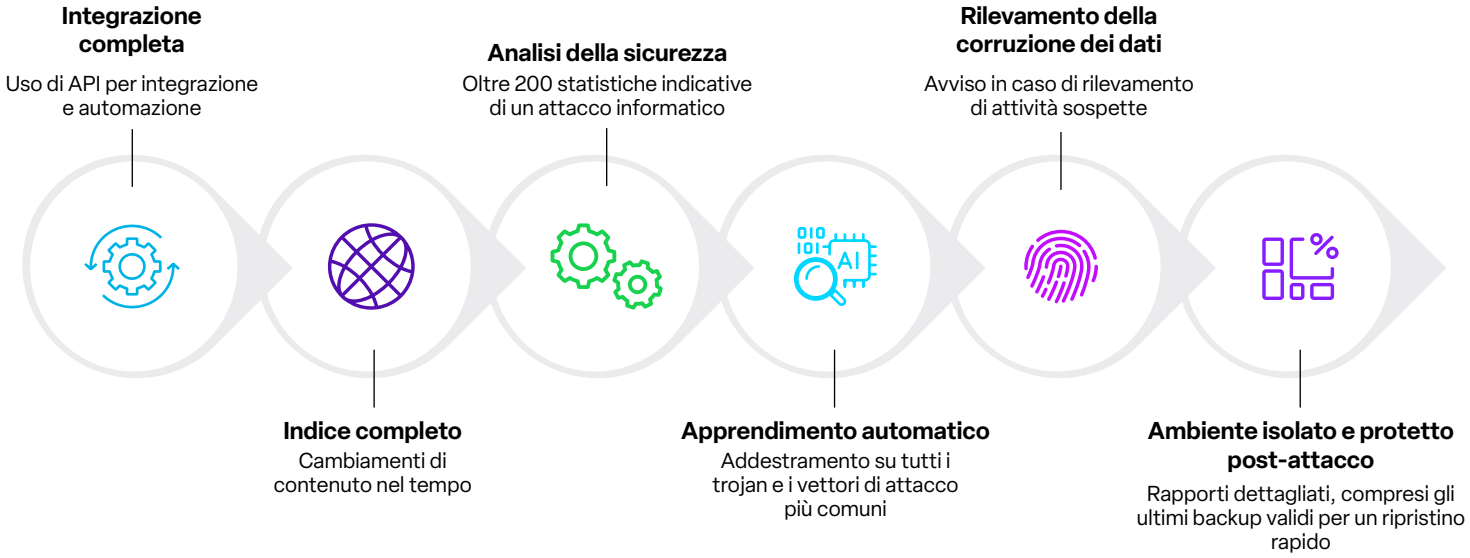


che ci aiutano a rendere i disastri informatici più facili da affrontare; tuttavia dobbiamo collegare i diversi elementi di queste soluzioni e orchestrare il processo, perché gli aggressori vogliono creare il caos e non lasciare il tempo di pensare.

Identificare, orchestrare e agire

Oggi le aziende presentano ambienti complessi e multilivello che comprendono molti strumenti, sistemi di monitoraggio e processi che, in molti casi, ruotano intorno a centri operativi di sicurezza (SOC) dedicati. All'interno del SOC esistono diverse applicazioni progettate per la sicurezza delle infrastrutture, tra cui molte etichettate come SIEM (Security Information and Event Management) e SOAR (Security Orchestration And Response). Gli ambienti SIEM e SOAR sono il punto centrale di raccolta di quasi tutto ciò che riguarda la sicurezza, non appena viene rilevato un problema. Il passo successivo consiste nel creare un processo ben definito e orchestrato che venga eseguito alla velocità di elaborazione senza la necessità di un lento intervento umano. Le frazioni di secondi contano e l'esecuzione quasi istantanea è fondamentale per avere la possibilità di limitare l'esposizione.

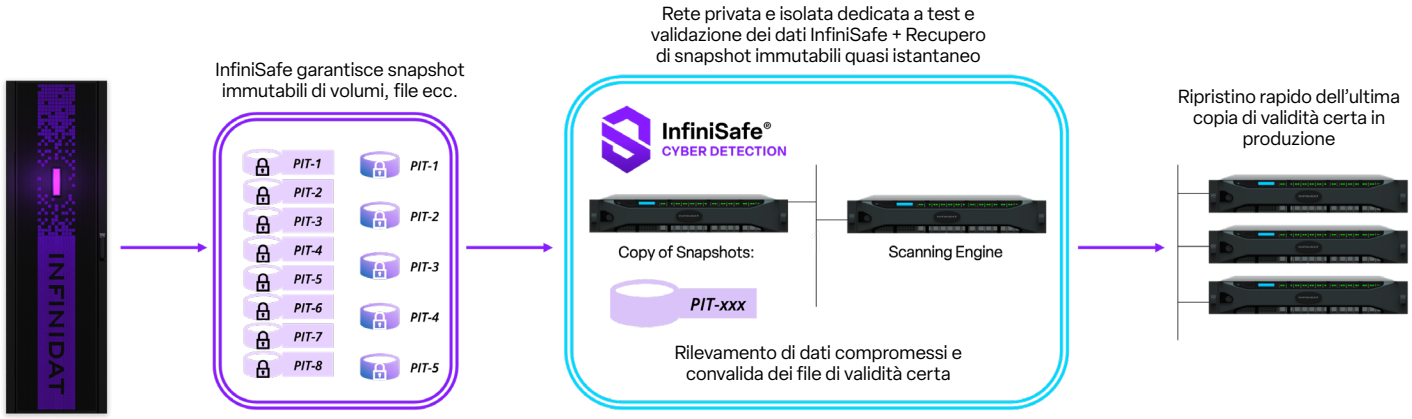
Come fa Infinidat a raggiungere questo obiettivo? Semplice. Da anni ormai i nostri prodotti sono dotati delle funzionalità InfiniSafe. Disponiamo di una potente architettura di riferimento InfiniSafe per la famiglia InfiniBox, facilmente estendibile e orchestrata per essere attivata da qualsiasi evento, ovunque. In questo caso, potrebbe essere attivata dagli ambienti SIEM o SOAR di un'azienda, che dispongono di interfacce estensibili, tramite API o CLI. Se vengono abbinati a un'architettura di riferimento InfiniSafe ben definita, questi ambienti applicativi creano



un insieme completamente automatizzato di funzionalità che possono essere orchestrate per creare in modo proattivo e rapido snapshot immutabili che proteggano le risorse di dati primarie più critiche.

Convalidare i dati e ripristinarli rapidamente

InfiniSafe è anche in grado di orchestrare la creazione di una rete privata e isolata dedicata a test e validazione dei dati, separata dalla rete o dai sistemi interni degli utenti eventualmente colpiti. È possibile (e consigliabile) disporre di una serie di risorse dedicate al di fuori della produzione per testare e convalidare i dati con gli strumenti e il software associato necessario. InfiniSafe può quindi presentare istantaneamente snapshot



immutabili di volumi o file system alla rete isolata, connetterle e utilizzare tutti gli strumenti a disposizione per convalidare i dati. Infinidat può aiutare anche in questo processo di convalida, grazie a strumenti potenti e smart.

InfiniSafe Cyber Detection è una soluzione aggiuntiva ai componenti altrimenti gratuiti di InfiniSafe. InfiniSafe Cyber Detection esegue una scansione approfondita degli archivi di blocchi, file e database presentando le snapshot immutabili di InfiniBox e InfiniBox™ SSA a un potente motore di scansione basato sull'intelligenza artificiale. La scansione serve a convalidare l'integrità dei dati e, grazie all'apprendimento automatico basato sull'intelligenza artificiale, a identificare eventuali modifiche dannose a seguito di un attacco informatico. Inoltre, utilizza più di 200 data point per individuare gli eventuali dati compromessi con una precisione del 99,99%. Questo livello di accuratezza e di dettaglio garantisce la massima definizione e la facilità di gestione di qualsiasi ulteriore analisi nell'ambiente protetto, riducendo al minimo i possibili falsi positivi, perché quando si ha a che fare con un evento informatico è fondamentale essere veloci e precisi. L'estensione di questa funzionalità a InfiniSafe Cyber Detection richiede l'acquisto di licenze specifiche per l'attività di scansione.

Sintesi

Se non si è preparati, i malintenzionati creano il caos e ottengono il controllo delle risorse di dati più critiche. Conoscere lo stato dei propri dati e mantenerli protetti in modo proattivo, non solo attraverso eventi programmati, è un fattore chiave per ridurre la finestra di minaccia, recuperare il vantaggio e fermare chi cerca di estorcere denaro compromettendo i dati.

italia@infinidat.com

Lenovo
INFINIDAT