LA SOLUZIONE IN BREVE

Ferma il ransomware con InfiniGuard® InfiniSafe®

LA SFIDA

Il ransomware è un software dannoso che prende in ostaggio i dati criptandoli.

In passato, le aziende con un processo di backup funzionante potevano ripristinare i dati non corrotti sui sistemi di produzione colpiti. Tuttavia, il codice dei ransomware diventa sempre più sofisticato e oggi attacca comunemente anche i backup. Le aziende subiscono, in media, un attacco ransomware ogni 11 secondi[1] quindi il vecchio approccio "se ci attaccano, ripristiniamo il backup" non è più sufficiente.

Le vittime non hanno buone opzioni tra cui scegliere. Alcune aziende decidono di pagare, e sono abbastanza fortunate da ottenere in cambio la chiave di crittografia. Molte, invece, pagano ma non ottengono nulla. Altre si affidano a costosi servizi di decrittografia e altre ancora usano un vero e proprio camion, per recuperare cartucce a nastro off-line e si preparano a un arduo processo di recovery.

Il costo? IDC stima che il ransomware costi alle imprese 20 miliardi di dollari all'anno. Questo numero cresce se si aggiungono le piccole e medie imprese, spesso obiettivi degli attacchi ransomware.

Il ransomware oggi

Nei primi mesi del 2021, il provider di sistemi di sicurezza informatica BlackFog[2] ha indicato alcuni dei principali incidenti informatici che si sono verificati: un attacco al Victor Central School District di New York ha criptato dati e sistemi e bloccato gli utenti. Tutte le scuole del distretto sono state costrette a chiudere. A marzo, il produttore di computer Acer è stato raggiunto da una richiesta di riscatto pari a 50 milioni di dollari per impedire agli hacker di pubblicare i dati sensibili rubati.

Ancora più recente è il famigerato attacco ransomware a Colonial Pipeline, che fornisce fino al 45% del carburante alla costa orientale degli Stati Uniti. L'attacco è stato sferrato da un gruppo di hacker russi e l'operatore dell'oleodotto ha dovuto spegnere in fretta i suoi sistemi per contenerne la diffusione. Nonostante questo, le stazioni di servizio in gran parte del paese hanno faticato a ottenere le forniture di carburante.

Anche le aziende più piccole vengono colpite. La società di sicurezza Infrascale ha stimato che il 46% delle piccole imprese ha subito attacchi ransomware e il 73% di esse ha riferito di aver pagato un riscatto. Queste richieste di riscatto potranno anche non raggiungere i 50 milioni di dollari, tuttavia sono costose e non forniscono alcuna garanzia che gli hacker manterranno la loro parola.

Salviamoci con il backup, forse

È ovviamente meglio che il backup sopravviva all'attacco ma ormai gli hacker sanno dove colpire e prendono di mira i sistemi di backup! Limitare la capacità di ripristinare non fa altro che rafforzare la loro posizione. I metodi tradizionali di backup e ripristino di emergenza non sono applicabili al cyber recovery e, di conseguenza, i tuoi piani devono considerare specifiche esigenze di ripristino informatico.

Tradizionalmente, il personale IT aumenta la velocità di backup utilizzando backup sintetici e storage deduplicati. Effettuare un recovery su larga scala in caso di attacco informatico significa, però, mettere insieme i dati provenienti da più backup diversi, con il risultato di un modello IO di lettura altamente casuale sullo storage di backend, il che determina tempi di recovery prolungati e un impatto potenzialmente grave sull'azienda.

Le caratteristiche e i vantaggi principali di InfiniGuard InfiniSafe includono:

- Ripristini rapidi di livello enterprise su scala petabyte
- Protezione del backup dagli attacchi informatici grazie a snapshot immutabili che non possono essere cancellati, criptati o modificati
- Possibilità di dimostrare la conformità normativa grazie al backup consolidato e a snapshot immutabili
- Supporto di più operazioni simultanee di backup e recovery senza impatto sulle prestazioni
- Convalida dell'ambiente di recovery
- I 3 nodi di deduplica ridondanti in una configurazione attiva/attiva/passiva proteggono i dati e garantiscono la riuscita delle operazioni di backup e recovery
- Riduzione di costi energetici e spese di gestione grazie al consolidamento del backup fino a 50PB
- Scalabilità estrema e supporto multiprotocollo per VTL, NFS, CIFS, OST, RMAN e DB/2
- Riduzione al minimo delle perdite economiche e dei danni alla reputazione ripristinando i dati in modo quasi istantaneo e sicuro
- Recupero dei dati senza compromettere l'integrità, qualunque sia la causa: attacchi informatici, malfunzionamenti tecnici, disastri naturali o errori umani

[1] Cybersecurity Ventures https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[2] BlackFog https://www.blackfog.com/the-state-of-ransomware-in-2021

INFINIDAT

LA SOLUZIONE: InfiniGuard con InfiniSafe

InfiniSafe, incluso in InfiniGuard, è la soluzione di protezione e recovery dati di Infinidat. InfiniSafe si aggiunge all'architettura di protezione dei dati di InfiniGuard, che consente il ripristino quasi istantaneo a una frazione del costo dei PBBA concorrenti. InfiniGuard utilizza InfiniBox multi-PB come backend e aggiunge un livello software innovativo per ottimizzare il layout dei dati per un ripristino rapido, senza sacrificare la velocità di backup.

L'innovativa tecnologia di InfiniGuard sfrutta un'ampio livello di memoria dinamica ad accesso casuale (DRAM) come cache primaria, insieme a un livello ancora più esteso di unità a stato solido (SSD) come cache secondaria. L'algoritmo proprietario TRIE (un albero di nodi al posto di un albero binario o di un algoritmo di hashing) predice i modelli di IO e sposta preventivamente in cache i dati per accelerare i tempi di backup e recovery.

Invece di provare a recuperare i dati da più appliance di backup, tipi di media e siti di archiviazione, InfiniGuard consolida più backup in una singola appliance facilmente gestibile che scala fino a 2PB di capacità utilizzabile e fino a 50PB di capacità effettiva. I ripristini paralleli da tutte le meccaniche dell'array contribuiscono ad aumentare la velocità di recovery.

InfiniSafe in dettaglio

Le capacità native di InfiniSafe di InfiniGuard portano protezione e recovery al livello successivo. InfiniSafe protegge dagli attacchi ransomware con quattro tecnologie che sono fondamentali per una soluzione di cyber recovery:

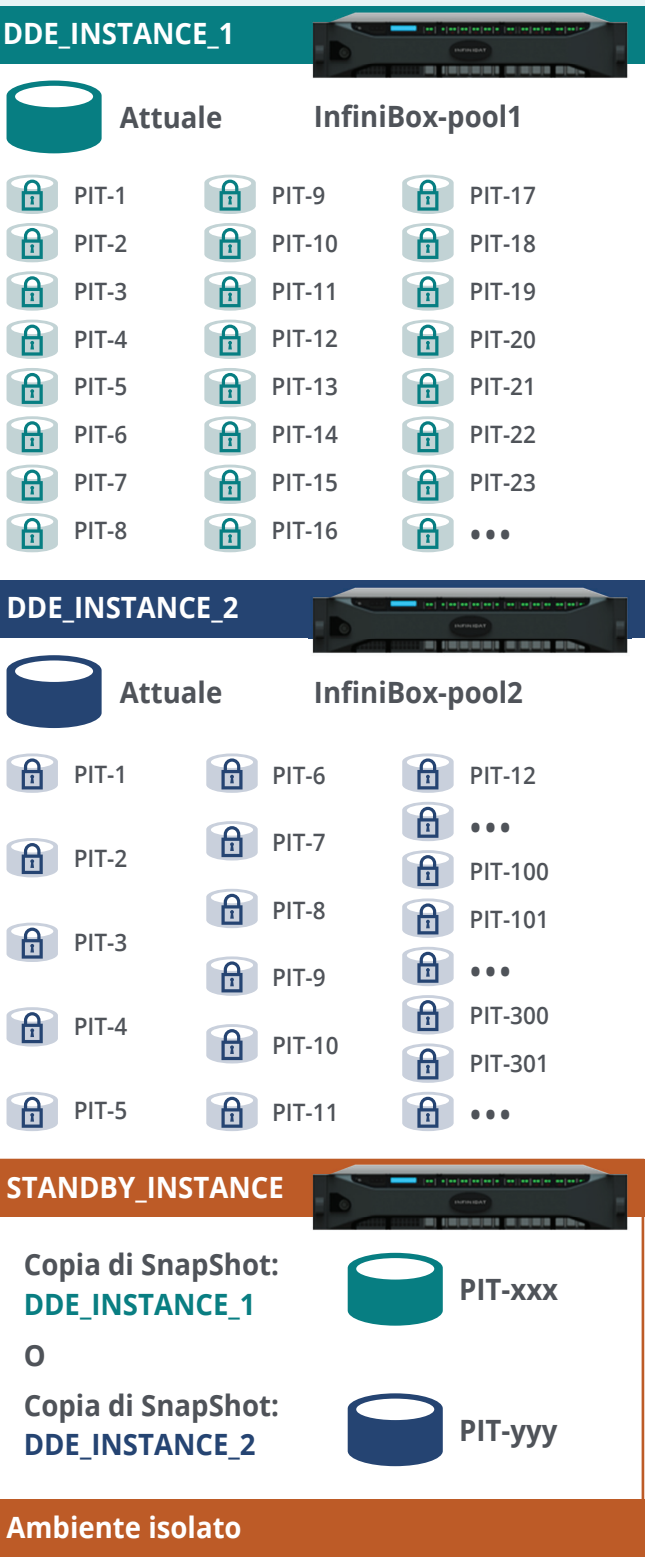
1. Immutable Snapshots

Le snapshot immutabili non possono essere eliminate o modificate. Il supporto di Infinidat collabora con i clienti per configurare le snapshot del sistema al fine di ottimizzare le esigenze di sicurezza, comprese le impostazioni di conservazione, le pianificazioni e le politiche associate. Non è possibile per un malintenzionato o un membro inesperto del personale IT modificare queste impostazioni o eliminare qualsiasi snapshot immutabile esistente.

2. Logical Air-Gapped Protection

La priorità è garantire che i dati da proteggere siano isolati da altre aree del sistema. Altre soluzioni richiedono lo spostamento dei dati mediante copia o replica in un sistema separato, aggiungendo costi e complessità. La tecnologia InfiniSafe lo fa localmente, risparmiando sui costi ed eliminando la complessità.

InfiniGuard con InfiniSafe protegge l'intero storage di backup tramite snapshot immutabili di Infinidat. Ogni motore di deduplica (DDE) può essere ripristinato in un punto diverso nel tempo. InfiniSafe o i test di individuazione possono essere attivati anche in un ambiente di standby.



[3] Indagine Infrascale 2020 https://www.infrascale.com/press-release/infrascale-survey-reveals-close-to-half-of-smbs-have-been-ransomware-attack-targets/

3. Rete privata ed isolata dedicata al test

Una rete completamente privata utilizzata per la convalida e il recupero dei dati.

4. Recupero quasi istantaneo

Rendere i dati disponibili il più rapidamente possibile è fondamentale quando si prova a ripristinare in caso di attacco. InfiniSafe ti consente di recuperare tutti i tuoi dati e renderli disponibili per il ripristino in pochi minuti, indipendentemente dalle dimensioni del repository di backup. Non pagherai alcuna penale.

Il ripristino diventa sistematico, veloce e verificabile, quasi istantaneo da qualsiasi punto della cronologia dei dati. Questo sistema isolato e semplice da usare permette alle aziende di verificare i dati prima di ripristinare l'ambiente operativo. Inoltre, questo ambiente supporta la convalida delle routine dei backup sicuri senza interrompere le operazioni di backup quotidiane, il tutto senza sistemi secondari e senza spostamento di dati.

SINTESI

Gli attacchi informatici sono una minaccia reale e in crescita e le aziende non dovrebbero sottovalutare le conseguenze potenzialmente dolorose. Purtroppo, gli attacchi informatici prenderanno di mira tutti gli ambienti di backup prima o poi! Pertanto, riducendo la tua capacità di rispondere in modo efficace sarà più facile attaccarti

In questo caso, è necesario essere più intelligenti. Adottare InfiniGuard con InfiniSafe per difendersi da minacce, attacchi informatici, guasti tecnici e disastri, oppure da semplici errori umani. InfiniGuard con InfiniSafe garantisce la sicurezza necessaria per recuperare rapidamente i dati e far tornare operativa la tua azienda.