SOLUTION BRIEF

Difendi i tuoi dati con InfiniBox®: Qualunque sia la minaccia - ransomware, disastro naturale, guasto al sistema, errore umano - InfiniBox ti copre le spalle.

LA SFIDA

Oggi, i dati vivono in un mondo che non è mai stato così pericoloso. I disastri naturali sono in aumento e un semplice errore umano può rendere assolutamente inutilizzabili volumi interi di dati preziosi. Inoltre, oggigiorno bisogna aggiungere gli attacchi informatici, come ransomware e malware, che sono tra i maggiori timori di CEO e CISO.

Se il quadro sembra drammatico e pericoloso, è perché effettivamente lo è... o potrebbe esserlo se si è impreparati. Per proteggere i dati da queste minacce, la maggioranza delle aziende utilizza gli strumenti tipici di protezione (backup). Molte attuano anche un business continuity plan a garanzia dell'affidabilità e della disponibilità dei dati nonostante le interruzioni e gli attacchi. Un piano di questo tipo è reso ancor più complesso dall'aumento di ransomware e malware.

Persino le aziende più evolute non sono sempre sicure di avere protetto a sufficienza i dati. Al fine di garantire una protezione dei dati all'avanguardia, che include la resilienza informatica e dei dati, InfiniBox e InfiniBox SSA di Infinidat forniscono la Reference Architecture InfiniSafe®, che consente di stabilire i processi corretti con strumenti e tecnologie ad hoc per dati sempre sicuri, disponibili e affidabili.

In questo Solution Brief prenderemo in esame una delle più comuni e pericolose minacce ai dati: l'attacco informatico e il ransomware.

> *"... il crimine informatico è diventato un problema così grave che nei recenti sondaggi di Fortune a maggio 2021 e di KPMG a marzo 2021, i CEO lo hanno messo al primo posto tra le minacce alle loro aziende."*

Aumento esponenziale del crimine informatico

- Non è una questione di SE, bensì di QUANDO si verrà attaccati e con quale frequenza. Oggi è inevitabile e tutte le aziende devono essere preparate.
- Il crimine informatico non si limita a un solo tipo di attacco. I più diffusi includono il phishing, il furto di proprietà intellettuale online e le truffe online (come l'onnipresente segretario generale delle Nazioni Unite che offre decine di milioni di dollari al fortunato destinatario).
- La realizzazione di sofisticati attacchi malware come quelli di tipo Advanced Persistent Threat (APT) richiede molte risorse, ma ricompensa ampiamente. Gli hacker APT mirano alle reti ricche di dati preziosi, al denaro e al rischio di grave imbarazzo pubblico nel caso in cui si verifichi un attacco.[1]
- In effetti, il crimine informatico è diventato un problema così grave che secondo i recenti sondaggi ai CEO condotti da Fortune a maggio 2021[2] e da KPMG a marzo 2021[3] è al primo posto tra le minacce alle aziende.
- È ampiamente documentato che gli attacchi informatici vengono eseguiti dopo mesi di pianificazione. I tempi medi di permanenza in cui gli intrusi si infiltrano nell'ambiente di un'azienda superano i 9 mesi.

Ransomware

Il ransomware è un tipo di malware. Tuttavia, diversamente dagli attacchi APT ad alto rischio/alto rendimento, gli hacker possono acquistare i

[1] "Cosa significa Advanced Persistent Threat?" Kaspersky
[2] "Fortune 500 CEO survey"
[3] "KPMG 2021 CEO Outlook Pulse Survey"
[4] "Revealed: I supermakert che venderanno malware per 50$" Forbes

ransomware sul dark web. In molti casi è economico e alcuni venditori intraprendenti lo affittano perfino; una pratica che ha creato il Cybercrime-as-a-Service (CaaS).[4]

Gli attacchi ransomware inseriscono un software che codifica automaticamente tutti i file e i volumi a cui riesce ad accedere. Se il ransomware attacca un computer in rete, il processo crittografico si diffonde su tutta la rete con conseguenze sullo storage primario e secondario, backup e archivi compresi. In molti casi lo storage secondario è il primo obiettivo, limitando la capacità di recupero dell'azienda e rafforzando la posizione degli intrusi. Quindi, gli hacker richiedono alle vittime un pagamento per rilasciare la chiave di decrittazione.

Perché non pagare?

Molte vittime preferiscono pagare un riscatto nella speranza di ottenere la chiave, piuttosto che perdere i dati.

Ovviamente, è una partita persa. Il report **"State of Ransomware 2021"** (Lo stato del ransomware 2021) di Sophos mostra i risultati della ricerca svolta sugli eventi ransomware: il 92% delle aziende che ha pagato un riscatto negli ultimi 12 mesi non ha recuperato tutti i dati. Secondo gli intervistati, i dati recuperati sono stati in media il 65%. Ne consegue che alcune aziende li hanno recuperati parzialmente, altre completamente e altre ancora per niente. Il report di Sophos ha inoltre rivelato che nella prima parte del 2021 il costo medio per il recupero è raddoppiato rispetto al 2020. In sostanza, il recupero può costare milioni di dollari.

> *"Sono sempre rimasto colpito dalle prestazioni, dal rapporto costi-benefici e dalla gestione dei sistemi adottato da OFFSITE... La funzionalità delle snapshot immutabili [di Infinidat] è un grande valore aggiunto nella protezione dei dati dal ransomware."*
>
> — **Chief Technology Officer**, OFFSITE

Inoltre, i governi di tutto il mondo stanno stabilendo norme, regolamenti e leggi in merito al pagamento di riscatti e alla segnalazione di incidenti. È importante che le aziende siano informate in merito ai requisiti nelle loro aree.

LA SOLUZIONE

InfiniBox, il potente sistema di storage di Infinidat, offre una soluzione basata su intelligenza artificiale che dopo la configurazione iniziale non necessiterà più di alcun intervento grazie a una disponibilità senza precedenti, prestazioni ineguagliate e un costo totale di proprietà notevolmente inferiore. Management e data plane distinti creano una poderosa protezione dei dati nell'architettura del sistema.

Le capacità di difesa di InfiniBox consentono una migliore protezione dei dati con snapshot/snapshot immutabili, funzioni di replica, crittografia e sistemi di controllo per la gestione degli accessi; rilevano più rapidamente le minacce con allarmi legati alle soglie di capacità del pool di storage e permettono un recupero più veloce grazie alle snapshot locali e replicate.

InfiniSafe: Architettura di riferimento per la famiglia InfiniBox

Comprendere come creare un ambiente con resilienza informatica per lo storage primario è più importante che mai. Le aziende hanno bisogno di una strategia su più livelli per proteggere le risorse più critiche. L'architettura di riferimento di InfiniSafe definisce metodologie facilmente implementabili ai fini dell'ottimizzazione della resilienza informatica. Alla base c'è l'approccio dei quattro pilastri:

- **Snapshot immutabili**
- **Air-gapping logico remoto**
- **Rete privata ed isolata dedicata al test e verifica dei dati**
- **Recovery praticamente istantaneo**

La creazione di copie protette e non modificabili dei propri dati è importantissima. Queste sono già dotate di logical air-gap; tuttavia, la procedura di propagazione mediante replica a una seconda copia immutabile è importante, proprio come il ripristino di emergenza. Quindi, bisogna testare e/o convalidare i dati della copia in questione. Una protezione perimetrale (definita anche zero trust) separa l'utente dalla produzione ed è attiva solo per il tempo necessario a convalidare quello che specificamente si vuole sia assolutamente protetto. L'utente è in grado di usare gli strumenti e le applicazioni migliori per la convalida e/o il test dei dati. Infine, una volta convalidate queste copie point in time, sarà possibile recuperare i dati in questione nel giro di pochi secondi o minuti. Utilizzando le capacità della nostra famiglia di prodotti, InfiniBox offre tutto questo senza esigenze proprietarie o vincoli con un particolare vendor o set di strumenti.

Snapshot: la colonna vertebrale della protezione dei dati e della business continuity

InfiniSnap®, il meccanismo delle snapshot di Infinidat, amplia le fondamentali capacità di protezione dei dati senza ripercussioni su scalabilità o prestazioni. InfiniSnap utilizza un meccanismo redirect-on-write senza bloccaggio che crea snapshot e snapshot immutabili consentendo un ripristino veloce on demand.

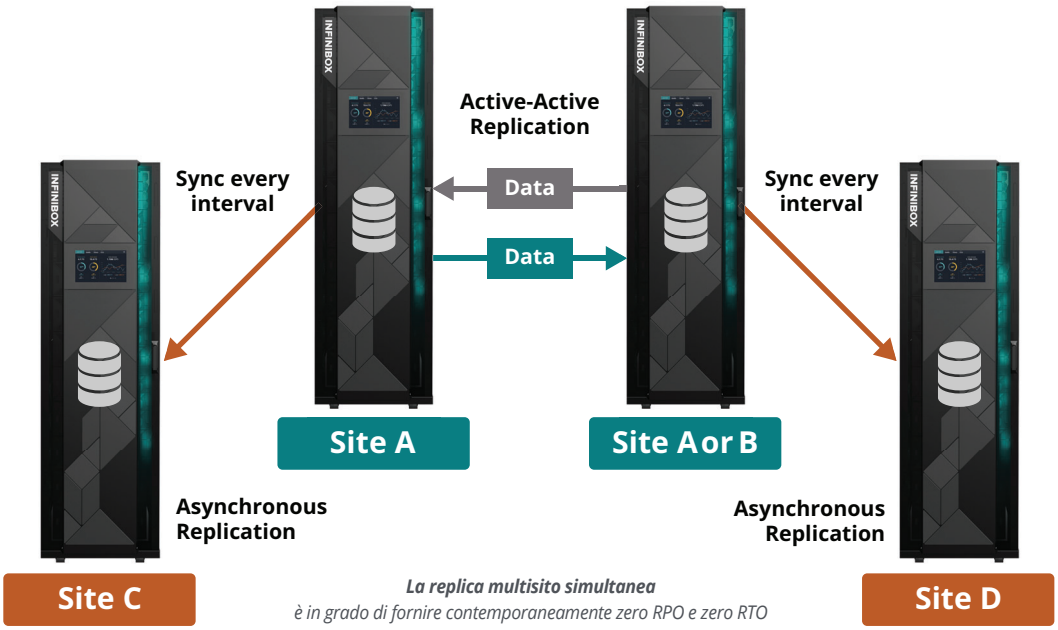
Le snapshot possono essere di sola lettura o scrivibili e ogni set di dati è in grado di archiviarne fino a 1000. Le snapshot di InfiniSnap consentono di ottenere snapshot immutabili per volumi, file system e gruppi di coerenza. La Snapshot Directory consente agli utenti finali di esplorare, selezionare e recuperare file inavvertitamente cancellati o modificati.

- **Snapshot immutabili:** le snapshot immutabili non possono essere modificate o cancellate entro un determinato periodo di conservazione. Sebbene gli amministratori possano prorogare la data di scadenza del blocco, non sono in grado di anticiparla. La funzione delle snapshot immutabili abilita anche snapshot nascoste come immagini di backup che proteggono ulteriormente le snapshot dagli attacchi.
- **Rilevamento delle minacce:** la crittografia ransomware aumenta le dimensioni dei dati, incrementando la dimensione delle snapshot dei dati. Gli amministratori possono impostare soglie di consumo della capacità che li avvisino qualora il volume delle snapshot superi improvvisamente i parametri medi. Nel caso rilevino un attacco, gli amministratori possono subito accedere ai dati, testarli e recuperarli in fretta dall'ultima snapshot utile.

Replica: potenziare la business continuity

La replica potenzia la capacità delle snapshot di proteggere e recuperare i dati minacciati. InfiniBox abilita vari tipi di replica in risposta a esigenze ambientali mutevoli.

- **Replica asincrona:** consente di raggiungere un RPO (Recovery Point Objective) di 4 secondi. Usando un'infrastruttura IP, riduce costi e complessità.
- **Replica sincrona:** permette un RPO di zero secondi con latenza inferiore a 400 microsecondi per applicazioni mission-critical. Se la WAN subisce un ritardo o un'interruzione, la replica sincrona di InfiniBox ritorna alla modalità asincrona. Quando la WAN viene ripristinata, il motore duplica automaticamente tutti i dati mancanti e la replica sincrona riprende senza interrompere le operazioni I/O.
- **Replica Active-Active:** i sistemi InfiniBox abilitano lettura e scrittura simultanee in gruppi di consistenza su aree metropolitane. I volumi sono immagini esterne che appaiono come percorsi multipli verso lo stesso volume. La replica sincrona mantiene sempre la coerenza dei volumi. Non esiste alcuna relazione master-slave e non sono necessari round-trip per eseguire aggiornamenti di scrittura sui volumi. Se necessario, un piccolo "witness" esterno può essere presente su un nodo standalone o una macchina virtuale su un cloud.
- **Replica multisito simultanea:** InfiniBox è in grado di replicare simultaneamente gruppi di consistenza dai siti principali a un altro sito in un'area metropolitana. Da lì, gli utenti possono effettuare la replica in modalità asincrona in terzo sito remoto.



La replica multisito simultanea è in grado di fornire contemporaneamente zero RPO e zero RTO in un'area metropolitana replicando i dati in modo asincrono su un terzo o quarto sito posizionato a distanza con RPO vicino allo zero.

INFINIDAT

Crittografia: Protezione dei dati crittografati

Il ransomware può ricodificare i file criptati, perciò le snapshot e la replica sono la prima linea di difesa. Ma più forte è la crittografia, più difficile sarà per gli hacker ricodificare i dati.

- **Convalida ai sensi dello standard Federal Information Processing Standards (FIPS) 140-2:** Il National Institute of Standards and Technology (NIST) ha assegnato la convalida FIPS 140-2 al modulo crittografico di Infinidat. Lo standard certifica InfiniBox per l'uso in una serie definita di progetti IT del governo degli Stati Uniti e dei settori regolamentati.
- **Self Encrypting Drives (SED) standard con crittografia AES-256:** InfiniBox usa lo standard Self Encrypting Drives (SED) con crittografia AES-256 conforme a FIPS 140-2, le chiavi di autenticazione più sicure in assoluto supportate dalle unità.
- **Key Derivation Functions KDF:** Infinidat usa una tecnologia KDF approvata dal governo federale degli Stati Uniti, che genera chiavi uniche al mondo per ogni unità. Il nostro pluggable key manager facilita la gestione esterna delle chiavi attraverso il Key Management Interoperability Protocol (KMIP).
- **Si integra con prodotti terzi:** mantiene una profonda integrazione con prodotti per la crittografia come Thales, VMware, Oracle TDE o Microsoft TDE senza programmazione specializzata o costi elevati.

Gestione degli accessi: divieto di accesso

Esistono diversi modi in cui i criminali informatici possono infiltrarsi in una rete. Le credenziali di amministratore sono sicuramente la via più apprezzata. InfiniBox è già configurato per impedire agli aggressori informatici di arrivare a questo punto: tutti gli accessi passano attraverso l'API che impedisce eventuali modifiche alle snapshot anche con le credenziali di amministratore.

Per cominciare, con la gestione degli accessi, gli aggressori non andranno lontano.

- **Controllo degli accessi basato sul ruolo (Role-based Access Control, RBAC):** nel control plane del sistema, il RBAC ha la funzione di proteggere account locali e dominio/gruppi LDAP. I ruoli assegnati a un gruppo consentono agli utenti di avere il controllo totale, il controllo su un pool di capacità limitata, oppure permessi di sola lettura. Gli utenti possono disabilitare o bloccare gli account locali, in modo che siano utilizzabili solo quando i tecnici di Infinidat eseguono attività di manutenzione. L'autenticazione basata su sessione protegge ulteriormente l'accesso alla gestione.
- **Autenticazione degli host:** iSCSI utilizza CHAP per autenticare gli host sul data plane. CHAP richiede l'autenticazione a più fattori per impedire a un host di accedere ai dati di un altro.
- **Integrazione con la gestione degli accessi di terzi:** Infinidat si integra con soluzioni esterne di classe enterprise per la gestione di accessi privilegiati quali CyberArk.
- **Accesso alla stazione di gestione e audit:** La gestione degli accessi comporta anche l'accesso alla Management Station attraverso un collegamento sicuro, mentre gli audit trail registrano tutte le operazioni che modificano la configurazione/lo stato o i componenti di una macchina. Le registrazioni di audit rilevano anche l'amministratore che ha apportato le modifiche alla configurazione.

CONCLUSIONE

La protezione dei dati è cruciale per il successo dell'azienda. L'insieme di ricche funzionalità di InfiniBox consente di sviluppare una resilienza completa per per i dati e per il sistema informatico, includendo lo storage nella strategia globale di sicurezza informatica dell'azienda.

Investendo in InfiniBox, non solo si ottengono prestazioni migliori, una disponibilità del 100%, una facilità di utilizzo che non richiede interventi dopo la configurazione e un costo totale di proprietà drasticamente più basso, ma si scoraggiano anche i potenziali aggressori ransomware. I criminali informatici si arricchiscono alle spalle di vittime impreparate. Non si aspettano certo di trovare poderose difese per la protezione dei dati.

Avvalendosi di snapshot immutabili, una replica potente, una crittografia sofisticata e una forte gestione degli accessi, InfiniBox respinge questi attacchi e lo fa con un modello all-inclusive personalizzato per il budget di storage, lo staff e gli obiettivi del cliente.