SOLUTION BRIEF

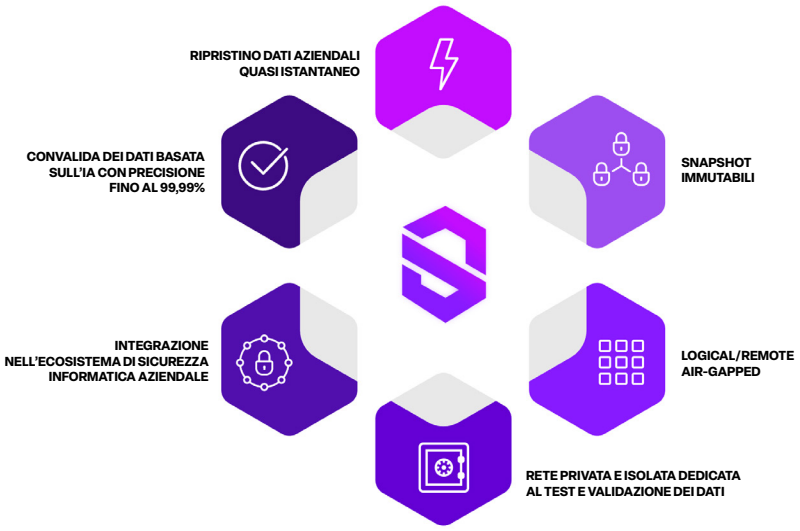
InfiniSafe® Cyber Detection

Si prevede che l'impatto della criminalità informatica costerà alle aziende 9.5 trilioni di dollari all'anno.[1] Ogni 39 secondi, si verifica un nuovo attacco sul web.[2] I costi per un'azienda includono il danneggiamento e la distruzione dei dati, la perdita di produttività, il furto di proprietà intellettuale, di dati personali e finanziari, l'appropriazione indebita e non solo. Oltre all'interruzione dell'attività dopo l'attacco, si aggiungono le indagini scientifiche, il rilevamento e il ripristino dei dati e dei sistemi violati e la perdita di fiducia e reputazione. La maggior parte dei team di sicurezza e IT ritiene che sia inevitabile subire un attacco informatico.
Sei pronto?

La nostra strategia di protezione e ripristino dei dati di nuova generazione è una strategia informatica incentrata sul ripristino. I servizi di cyber resilience della nostra piattaforma InfiniVerse®, forniti dalla gamma InfiniSafe, supportano direttamente ampie capacità di archiviazione informatica, offrendo protezione, prevenzione, rilevamento e capacità di ripristino garantiti completi ed end-to-end. InfiniSafe è un sistema "secure-by-design" (sicuro per progettazione) che comprende lo stack informatico di base, InfiniSafe Automated Cyber Protection (ACP) e InfiniSafe Cyber Detection.

InfiniSafe Cyber Detection potenzia le capacità di resilienza e risposta del cyber stack di Infinidat, consentendo ai team di sicurezza e IT di rilevare gli attacchi ransomware e malware con un'accuratezza fino al 99,99% e di consentire il ripristino quasi istantaneo dei dati da copie pulite di validità certa sulle piattaforme InfiniBox® e InfiniBox™ SSA.
In questo modo si può ribaltare la situazione a proprio favore.

InfiniSafe Cyber Detection aggiunge allo stack informatico di InfiniSafe un livello di rilevamento dei dati che circonda i suoi quattro livelli principali e amplia ulteriormente la capacità di InfiniSafe di individuare gli incidenti informatici. InfiniSafe Cyber Detection esegue una scansione approfondita dei datastore di blocchi, file e database presentando snapshot immutabili di InfiniBox e InfiniBox SSA a potenti motori di scansione basati sull'intelligenza artificiale che ne convalidano l'integrità e, attraverso il machine learning, identificano eventuali modifiche dannose che potrebbero indicare un attacco informatico.



InfiniSafe ACP si integra direttamente con le tue attività di sicurezza. Quando viene rilevato un attacco vengono eseguite automaticamente snapshot immutabili, le quali vengono presentate a InfiniSafe Cyber Detection che esegue una scansione approfondita e fornisce un'ampia reportistica analitica scientifica per diagnosticare quali dati siano stati compromessi e la natura della compromissione. In questo modo è possibile capire da dove provengono i dati compromessi. Quindi, grazie alla potenza della tecnologia InfiniSafe, l'utente può ripristinare rapidamente le normali attività aziendali, una volta identificata una copia dei dati della cui validità è certo.

Il 65% dei professionisti nel settore IT e sicurezza informatica intervistati indica il ransomware tra le prime 3 minacce alle proprie organizzazioni

Report ESG: 2023 Ransomware Preparedness

Rilevamento

Rilevamento analitico e basato sul machine learning

Analisi scientifica

Rapporti basati sull'analisi scientifica per diagnosticare e identificare la portata dell'attacco

Ripristino

Offre un report sull'ultima versione valida dei file per ottimizzare il ripristino

InfiniSafe Cyber Detection si avvale di una combinazione di oltre 200 analisi avanzate basate sul contenuto completo, che esaminano a fondo file e dati, andando oltre la semplice analisi dei metadati. Grazie a sofisticati algoritmi di machine learning, non è necessario conoscere in anticipo ogni nuova variante di minaccia. La profondità dell'analisi consente di rilevare varianti e tecniche di crittografia, sia note che sconosciute, identificando ogni comportamento sospetto. Nel caso di minacce già conosciute, il sistema è in grado di riconoscere la variante specifica utilizzata per tentare la compromissione, anche in assenza di una denominazione esplicita, con un'accuratezza del 99,99%. Questo aiuta le aziende a proteggere l'infrastruttura e i contenuti importanti dal punto di vista commerciale senza dare origine a un gran numero di falsi positivi, per concentrarsi sulle aree realmente problematiche e risolvere i problemi rapidamente. Se a questo si aggiunge l'ampia automazione e orchestrazione e l'integrazione della sicurezza con InfiniSafe ACP, si ottiene una delle soluzioni di cyber resilience dello storage end-to-end più complete a disposizione.

Rilevamento
InfiniSafe Cyber Detection utilizza l'analisi dei contenuti completi per tutti i dati protetti. Questa consapevolezza profonda è l'unico modo per essere sicuri che i tuoi dati siano integri e che i criminali informatici non stiano aggirando i tuoi strumenti di analisi dei dati, nascondendo le loro tracce e corrompendo segretamente i tuoi dati.

Proprio come nel machine learning della cache neurale nella nostra piattaforma InfiniBox, InfiniSafe Cyber Detection è dotato di un machine learning potente e deterministico. Combina oltre 200 analisi - una quantità oltre 20 volte maggiore rispetto ai concorrenti - a osservazioni di dati che, sommandosi, diventano più intelligenti nel tempo. Il machine learning è addestrato su migliaia di infezioni da ransomware, malware e trojan per trovare modelli di comportamento insoliti e distinguere l'attività dell'utente dal ransomware, riducendo al minimo i falsi positivi e negativi.

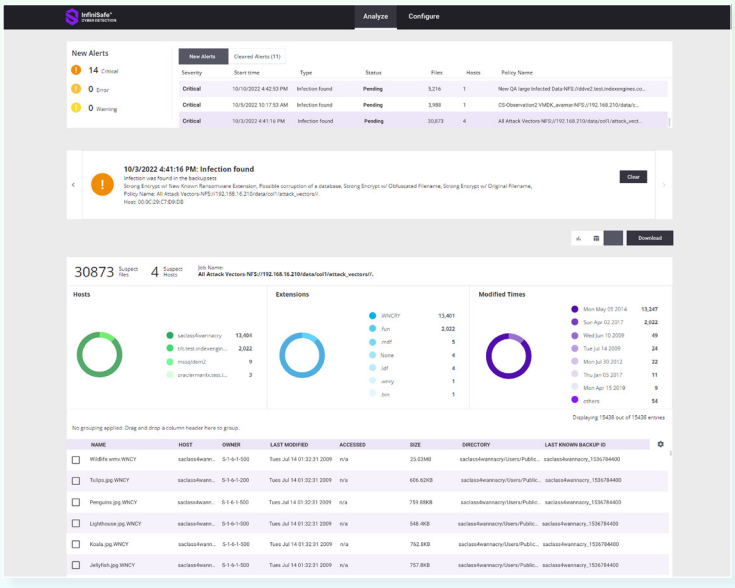
Analisi scientifica
Quando i dati sono danneggiati, InfiniSafe Cyber Detection genera un elenco dei file corrotti. I file vengono etichettati e vengono creati rapporti di analisi scientifica che consentono di diagnosticare e identificare la portata dell'attacco e fornire le informazioni necessarie per facilitare il ripristino.

Allarmi suddivisi per livello di severità

Nuove segnalazioni di corruzione dati

Grafici dinamici e personalizzabili per approfondire i dettagli dell'attacco

Report dei file corrotti disponibile per il download

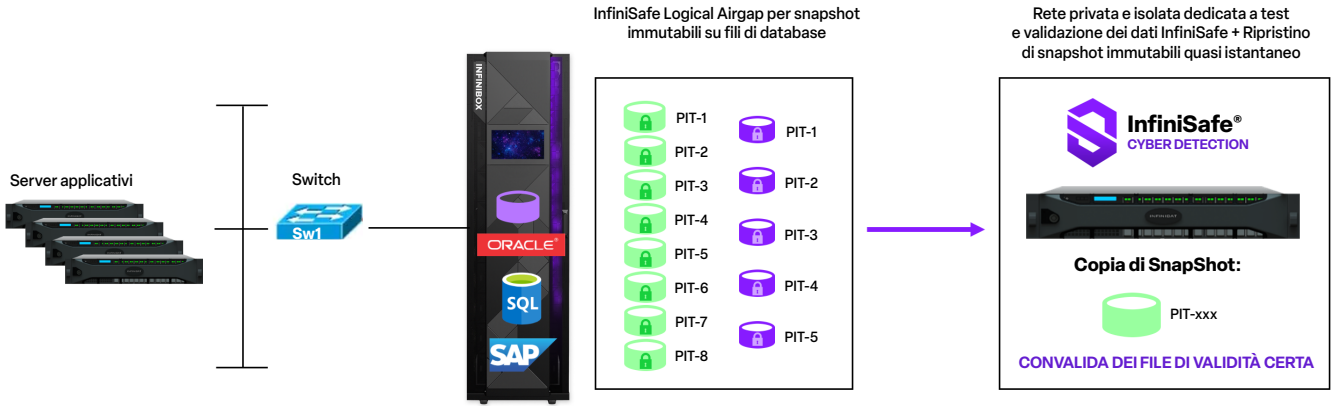


Dashboard post-attacco: esperienza d'uso migliorata, maggiore comprensione dei dati, flusso di lavoro post-attacco intuitivo.

Ripristino

Infine, InfiniSafe Cyber Detection segnala l'ultima copia di un file o di un backup della cui validità si è certi quando la copia di backup risiede su InfiniBox o InfiniBox SSA. Sa dove si trovano i dati danneggiati e la loro ultima versione valida e quali sono le snapshot o i set di backup che contenevano i dati per semplificare il processo di ripristino.

Casi d'uso: Rilevamento informatico di blocchi, file e database



Le aziende che utilizzano InfiniBox o InfiniBox SSA per le applicazioni di database mission-critical possono avere la certezza che utilizzando la tecnologia cyber stack InfiniSafe con Cyber Detection possono eseguire frequenti snapshot immutabili per convalidarne l'integrità e, attraverso il machine learning identificare qualsiasi modifica che indichi un attacco informatico. InfiniSafe Cyber Detection determina eventuali problemi e segnala le copie valide dei dati per un ripristino quasi istantaneo con InfiniSafe.

Cyber Detection Array

Le aziende che utilizzano soluzioni InfiniBox o InfiniBox SSA multiple possono replicare i dati in un Cyber Detection Array designato, in una rete privata e isolata dedicata a test e validazione dei dati, utilizzando gli strumenti di replica nativi di Infinidat. Il Cyber Detection Array eseguirà la scansione di tutti i file di dati, etichetterà i file corrotti e creerà un rapporto di analisi scientifica. Questa configurazione fornisce alle aziende le informazioni necessarie per rilevare un attacco informatico.

Gli incidenti causati da ransomware e malware continuano a interrompere i servizi e le attività critiche, dalle condutture energetiche alle scuole, passando per gli ospedali. Le perdite economiche totali dovute ad attacchi ransomware e malware sono in costante crescita. L'implementazione di una strategia efficace di protezione e ripristino dei dati di nuova generazione può ridurre l'esposizione dell'azienda e garantire un rapido ripristino.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

italia@infinidat.com

SB-CYBERD-250528-IT | © 2026 Infinidat, una empresa de Lenovo

Lenovo INFINIDAT