SOLUTION BRIEF

INFINIDAT

InfiniSafe® Cyber Detection

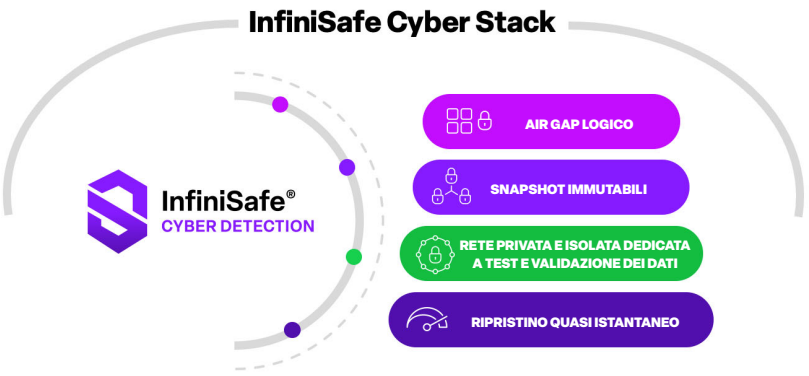
Si prevede che l'impatto della criminalità informatica costerà alle aziende 8 trilioni di dollari americani all'anno.[1] Ogni 39 secondi, si verifica un nuovo attacco sul web.[2] I costi per un'azienda includono il danneggiamento e la distruzione dei dati, la perdita di produttività, il furto di proprietà 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. Siete pronti?

La tecnologia InfiniSafe fornisce uno stack informatico a più livelli per la creazione di ambienti resilienti per il cyber storage con le piattaforme InfiniBox® e InfiniBox™ SSA.

L'introduzione di InfiniSafe Cyber Detection migliora le capacità di risposta e resilienza del cyber storage di Infinidat, consentendo ai team di sicurezza e IT di rilevare gli attacchi ransomware e malware con un'accuratezza che arriva fino al 99,5% e di consentire il recupero quasi istantaneo dei dati da copie pulite della cui validità si è certi sulle piattaforme InfiniBox e InfiniBox SSA.

InfiniSafe Cyber Detection aggiunge un livello di rilevamento dei dati allo stack informatico di InfiniSafe 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 degli archivi 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 l'apprendimento automatico, identificano eventuali modifiche dannose che potrebbero indicare un attacco informatico.

Quando viene rilevato un attacco, InfiniSafe Cyber Detection fornisce una reportistica di analisi scientifica per individuare i dati che sono stati compromessi e la natura del danneggiamento, oltre a fornire informazioni fondamentali sulla provenienza dei 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.



InfiniSafe Cyber Detection utilizza una combinazione di oltre 200 analisi basate sul contenuto completo che ispezionano il contenuto di file e dati, non solo i metadati. Potenti algoritmi di apprendimento automatico indicano il tipo di variante utilizzata per corrompere i dati con un'accuratezza del 99,5% e in questo modo aiutano le aziende a proteggere l'infrastruttura e i contenuti esigenti senza dare origine a un gran numero di falsi positivi. Questo consente loro di concentrarsi sulle aree realmente problematiche e risolvere i problemi rapidamente.

Se viene stabilito che i dati sono stati effettivamente corrotti, InfiniSafe Cyber Detection fornisce gli strumenti di analisi scientifica necessari per diagnosticare, identificare e aiutare a ripristinare le risorse interessate. InfiniSafe Cyber Detection segnala i file interessati dal problema mentre i risultati dell'indagine scientifica possono essere analizzati dai team di sicurezza e software che potranno eliminare eventuali problemi con gli strumenti a loro disposizione. I dati compromessi possono essere facilmente sostituiti con l'ultima versione della cui validità si è certi, per garantire il ritorno alla normalità delle attività aziendali con tempi di inattività minimi. InfiniSafe Cyber Detection è un'opzione aggiuntiva alla nostra tecnologia principale InfiniSafe ed è una licenza in abbonamento.

> "Il**79%** delle organizzazioni dichiara che la **preparazione al ransomware** è una delle prime cinque **priorità aziendali** complessive agli occhi del team esecutivo e/o del consiglio di amministrazione".
>
> Rapporto di ricerca di Enterprise Strategy Group, The Long Road Ahead to Ransomware Preparedness, giugno 2022

Rilevamento

Rilevamento analitico e basato sull'apprendimento automatico

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

Se vengono individuati dati corrotti, InfiniSafe Cyber Detection fornisce gli strumenti scientifici necessari per diagnosticare, identificare e aiutare a ripristinare le risorse interessate. InfiniSafe Cyber Detection segnala i file interessati dal problema mentre i risultati dell'indagine scientifica possono essere analizzati dai team di sicurezza e software che potranno eliminare eventuali problemi con gli strumenti a loro disposizione. I dati compromessi possono essere facilmente sostituiti con l'ultima versione della cui validità si è certi, per garantire il ritorno alla normalità delle attività aziendali con tempi di inattività minimi. InfiniSafe Cyber Detection è un'opzione aggiuntiva alla nostra tecnologia principale InfiniSafe ed è una licenza in abbonamento. InfiniSafe Cyber Detection è un prodotto post-attacco che si concentra sulla resilienza dei dati nel cyber stack InfiniSafe e non sostituisce le migliori prassi di prevenzione di ransomware e malware e i prodotti tradizionali di gestione delle minacce della parte relativa a server, applicazioni e networking della strategia complessiva di sicurezza informatica.

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 vostri dati siano integri e che i criminali informatici non stiano aggirando i vostri strumenti di analisi dei dati, nascondendo le loro tracce e corrompendo segretamente i vostri dati.

Analogamente a quanto avviene con la Neural Cache, InfiniSafe Cyber Detection è dotato di un apprendimento automatico potente e deterministico che abbina oltre 200 analisi - una quantità oltre 20 volte maggiore rispetto ai concorrenti - a osservazioni di dati che, sommandosi, diventano più intelligenti nel tempo. L'apprendimento automatico 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

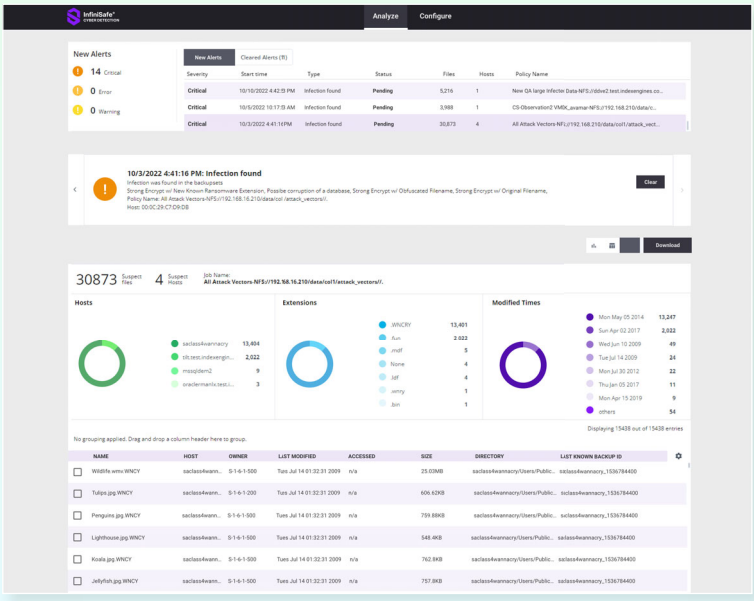
Quando i dati sono danneggiati, InfiniSafe Cyber Detection genera un elenco dei file corrotti. I file vengono etichettati e vengono creati rapporti di analisi scientifica che consentono di diagnosticare e identificare la portata dell'attacco e fornire le informazioni necessarie per facilitare il ripristino.

Avvisi organizzati per gravità

Nuovi dettagli sui sospetti di corruzione

Grafici dinamici e personalizzabili per approfondire i dettagli dell'attacco

Elenco dei file corrotti che può essere scaricato

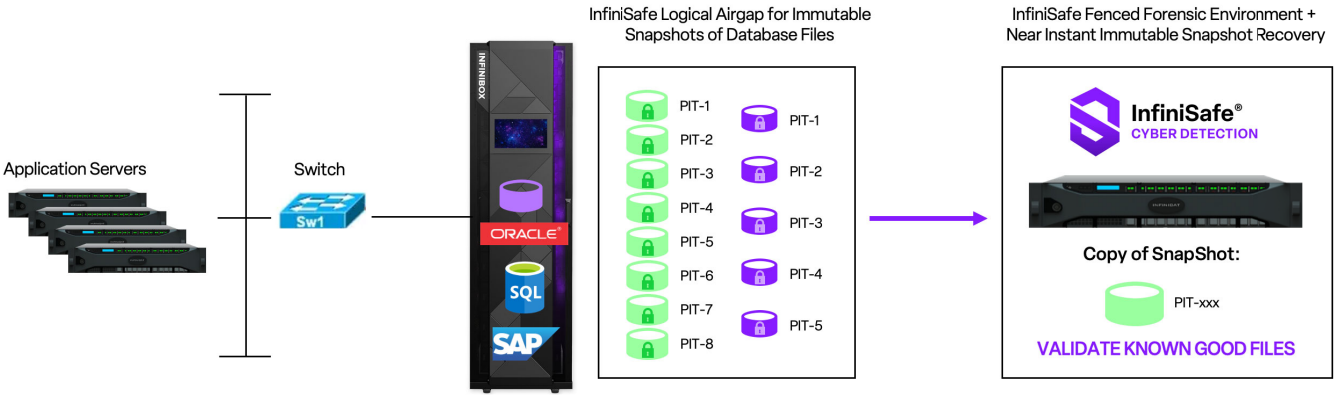


Dashboard post-attacco: esperienza d'uso migliorata, maggiore comprensione dei dati, flusso di lavoro post-attacco intuitivo.

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. Saprà 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 l'apprendimento automatico, identificare qualsiasi modifica che indichi un attacco informatico. InfiniSafe Cyber Detection determinerà eventuali problemi e segnalerà 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 rilevamento informatico può ridurre l'esposizione dell'azienda e garantire un rapido ripristino.

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
[2] https://techjury.net/blog/how-many-cyber-attacks-per-day/

italy@infinidat.com

INFINIDAT