rubrik

Ransomware Investigation

Rilevamento del ransomware e ripristino dell'operatività

GLI ATTACCHI RANSOMWARE SONO UNA REALTÀ

Gli attacchi ransomware stanno diventando sempre più diffusi e più costosi. In questo scenario, non è facile adottare la difesa perimetrale perfetta per fronteggiarli. Di fronte a questa sfida, le aziende cercano di adottare una strategia di risposta al ransomware olistica e multilivello che integri rilevamento, analisi e rapidità di ripristino.

Global ransomware damages predicted to reach

$265 billion

in 2031

Every **2** seconds

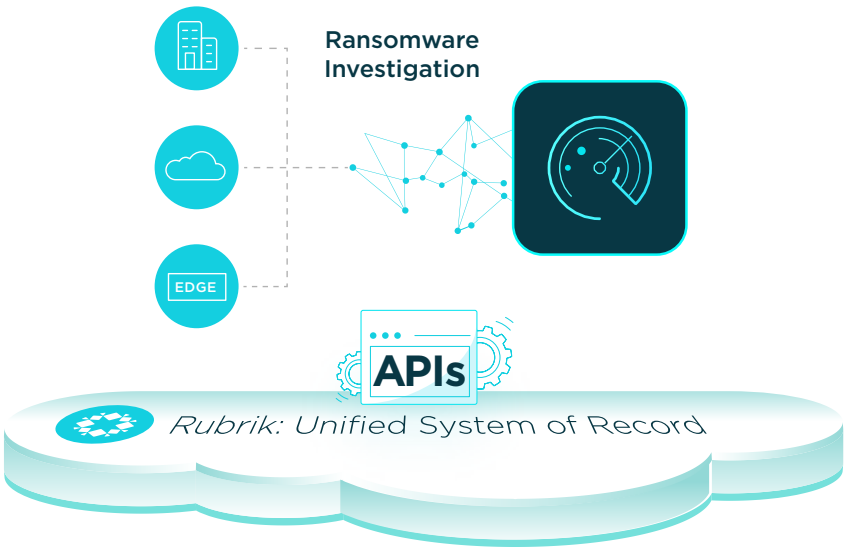
a ransomware attack on businesses predicted in 2031

Fonte: Cybersecurity Ventures

La strategia più efficace per prevenire un attacco ransomware e ripartire è la difesa in profondità. Un approccio basato su tecniche di difesa in profondità mantiene i backup al sicuro dal ransomware, identifica una situazione di attacco e velocizza il ripristino per ridurre al minimo l'impatto sul business.

RANSOMWARE INVESTIGATION: RIPRISTINO PIÙ VELOCE. INTELLIGENZA AVANZATA.

Ransomware Investigation consente di migliorare la resilienza contro il ransomware semplificando e velocizzando il processo di ripristino dopo un attacco. Ransomware Investigation favorisce ***un ripristino più rapido*** fornendo un'interfaccia semplice e intuitiva che consente di monitorare le modifiche dei dati nel tempo. La soluzione, infatti, sostituisce i ripristini manuali con una semplice procedura in pochi click per ridurre al minimo l'impatto sul business. Inoltre, ***migliora l'intelligenza*** utilizzando il machine learning per monitorare e generare in maniera proattiva avvisi in caso di attività sospetta.



ACCELERA IL RIPRISTINO

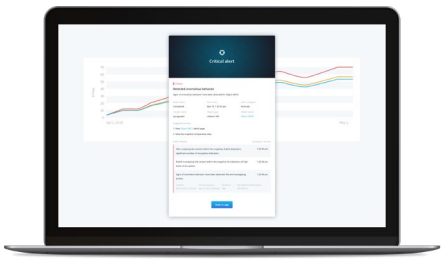
Riduci al minimo il downtime. Ripristina all'ultima versione non compromessa in pochi click.

AUMENTA L'INTELLIGENZA

Sfrutta il machine learning per rilevare i comportamenti anomali e inviare i relativi avvisi.

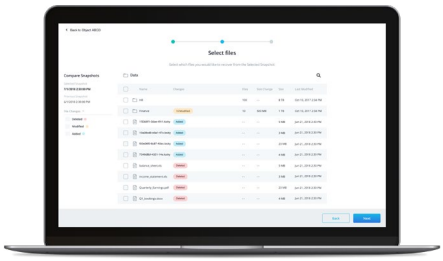
Analizza come sono stati modificati i tuoi dati per individuare rapidamente quali sono stati compromessi.

UNA DIFESA SU PIÙ LIVELLI: COME FUNZIONA RANSOMWARE INVESTIGATION



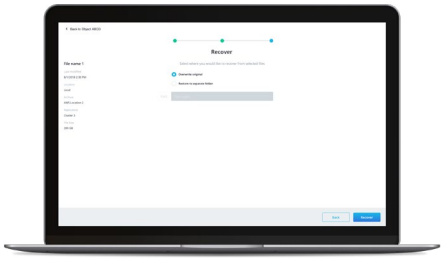
RILEVAMENTO DELLE ANOMALIE MEDIANTE IL MACHINE LEARNING

Ransomware Investigation sfrutta algoritmi di machine learning sui metadati delle applicazioni per stabilire una linea di riferimento base per ciascuna macchina. La soluzione esegue proattivamente il monitoraggio del sistema considerando i modelli di comportamento e segnalando qualunque attività che si discosti in modo significativo dalla linea di riferimento base. Ransomware Investigation analizza le diverse proprietà dei file, tra cui il change rate, le dimensioni anomale dei sistemi e le modifiche dell'entropia. Una volta rilevata un'anomalia, Ransomware Investigation ti avvisa del comportamento insolito tramite l'interfaccia utente di Rubrik, e-mail o applicazioni SOAR e SIEM come Cortex XSOAR di Palo Alto Networks. Grazie al machine learning, Ransomware Investigation può perfezionare continuamente il proprio modello di rilevamento delle anomalie nel tempo e prevenire le minacce più avanzate.



ANALISI DELL'IMPATTO DELLE MINACCE CON LA DATA INTELLIGENCE

Ransomware Investigation esegue la scansione continua dell'intero ambiente per fornire informazioni sulle modifiche intervenute sui dati nel tempo. In caso di attacco, le visualizzazioni semplici e intuitive permettono di individuare rapidamente le applicazioni e i file che sono stati modificati, nonché la loro posizione. Utilizzando l'interfaccia utente, è possibile scorrere l'intera gerarchia di cartelle ed eseguirne il drill-down per analizzare a livello di file quali sono stati aggiunti, eliminati o modificati. Con Ransomware Investigation puoi ridurre al minimo il tempo impiegato per scoprire ciò che è successo e quali dati sono andati perduti, con visibilità di dettaglio dei file più recenti non compromessi.



RAPIDO RIPRISTINO PER RIDURRE AL MINIMO L'IMPATTO SUL BUSINESS

La semplice esperienza utente di Ransomware Investigation si basa sull'interfaccia di gestione globale di Rubrik. Al termine dell'analisi, puoi selezionare semplicemente tutte le applicazioni e i file interessati, specificare il percorso desiderato ed eseguire in pochi click il ripristino alle ultime versioni non compromesse. Rubrik automatizza la restante parte del processo di ripristino, mentre gli utenti possono monitorarne l'avanzamento mediante l'interfaccia utente. Poiché Rubrik acquisisce i dati in un formato immutabile, il ransomware non può accedere ai backup e non può cifrarli o eliminarli.

COSA DICONO DI NOI I NOSTRI CLIENTI

"Quando siamo stati colpiti da un attacco ransomware alcuni anni fa, abbiamo utilizzato il ripristino rapido e le API di Rubrik per tornare operativi in meno di un'ora e senza alcuna perdita di dati. Oggi il ransomware è molto più sofisticato di quanto non fosse alcuni anni fa. Abbiamo potuto sfruttare la data intelligence di Ransomware Investigation per ricevere avvisi su comportamenti sospetti e per avere visibilità di dettaglio dei dati compromessi." **- Paul LaValley** Ex CIO, Yuba County, California

"I backup sono una delle difese più importanti, se non la più importante, contro il ransomware. Il file system di Rubrik è stato creato in modo da essere immutabile, il che significa che i backup non possono essere cifrati o eliminati dal ransomware. Ho la grande fortuna di poter affermare che siamo riusciti a recuperare il 100% dei dati in nostro possesso." **- Matthew Day** CIO, Langs Building Supplies

"Ransomware Investigation ci aiuterà a proteggere i nostri profitti e potrebbe farci risparmiare milioni di euro nell'eventualità di un attacco. Se non avessimo avuto Ransomware Investigation, non avremmo potuto sottoscrivere un'assicurazione cyber risk." **- Fabrice De Biasio** CIO, ASL Airlines

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

20220210_v2