SOLUTION BRIEF

5 mosse per contrastare il ransomware nel settore sanitario

Proteggi i pazienti e il tuo business con la data protection moderna di Pure Storage®.

Di recente si sono verificati attacchi ransomware che hanno paralizzato diversi ospedali a livello globale. Le previsioni indicano che gli attacchi al settore sanitario sono in costante aumento. Cybersecurity Ventures si aspetta un nuovo attacco ransomware ogni 2 secondi entro la fine del 2031.

Il tempo di recupero dal ransomware influisce sulla cura dei pazienti

Un attacco ransomware disattiva il sistema dei fascicoli sanitari elettronici (EHR) dell'ospedale colpito, con ripercussioni sull'interruzione delle attività su più fronti. Il downtime del sistema EHR ostacola le decisioni cliniche, causa potenziali errori medici e può persino rivelarsi una delle cause che determinano la morte del paziente.

Gli attacchi ransomware alle organizzazioni sanitarie decrittografano non solo i database di produzione degli EHR, ma anche i backup usati per il recupero dagli attacchi. Per far fronte alla crescente sofisticazione degli attacchi, le organizzazioni sanitarie devono adottare una strategia di protezione moderna di prevenzione e recupero dal ransomware.

Aumenta la protezione informatica con un framework in cinque passaggi

- Migliora la visibilità
- Garantisci il controllo
- Riduci l'esposizione
- Rendi gli attacchi più costosi
- Rispondi alle minacce ed evolviti

Recupero dal ransomware

Pure FlashBlade® con le snapshot SafeMode™ accelera il recupero dal ransomware aumentando le strategie di data protection.

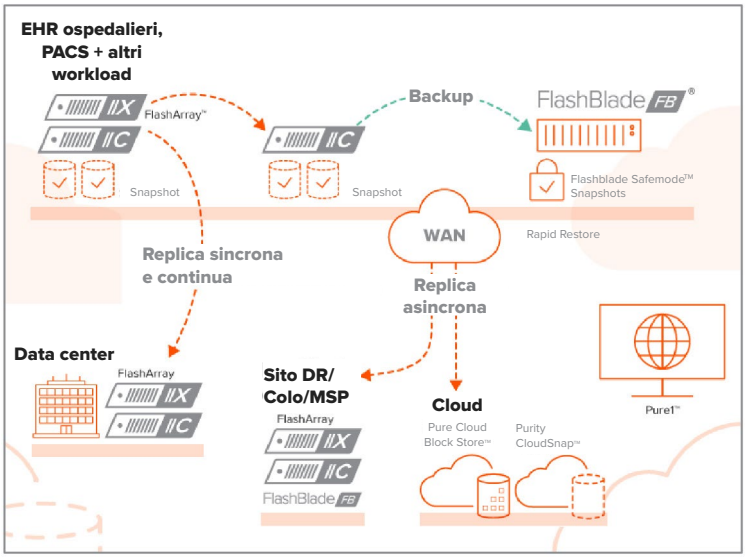
Data protection

Porta la tua organizzazione nel mondo della data protection moderna e abbandona le soluzioni legacy in silos.

Backup e restore

L'architettura moderna di Pure esegue il backup e il restore dei dati proprio quando è la cosa più importante da fare.

Ecco le cinque mosse che puoi fare per proteggere i dati contro gli attacchi informatici, e come Pure può esserti di aiuto:



Passaggio 1: Migliora la visibilità. Innanzitutto devi conoscere le dotazioni dell'ospedale e i motivi per cui sono installate. Quel server che nessuno sa perché si trovi nel seminterrato dell'ospedale potrebbe essere l'anello più debole della catena. È essenziale fare un inventario degli asset e dei punti di ingresso e monitorare gli eventi per ciascun asset, al fine di individuare le anomalie che possono indicare un'avvenuta intrusione.

- La piattaforma di analytics Pure1 Meta® sintetizza l'intelligence da migliaia di dispositivi.
- La combinazione di FlashBlade® di Pure con Splunk o Elasticsearch crea una piattaforma di sicurezza e data analytics potenti.

Passaggio 2: Garantisci il controllo. Delinea un perimetro di difesa virtuale intorno alla tua infrastruttura per controllare gli accessi. L'aumento della forza lavoro distribuita e le politiche di lavoro da remoto richiedono un nuovo approccio alla protezione informatica. Pure ha realizzato FlashArray™ da zero per eseguire la VDI più rapidamente e con una densità aumentata rispetto a qualsiasi altro prodotto sul mercato.

Passaggio 3: Riduci l'esposizione. Questo passaggio non riguarda solo la detection, ma anche la creazione di un ambiente con manutenzione e monitoraggio costanti, che richiedono la raccolta di enormi quantità di dati per analytics complessi. Ecco perché è importante disporre di un'infrastruttura la cui architettura garantisca risultati rapidi.

- Esegui la valutazione per sapere se la tua organizzazione è pronta ad affrontare il prossimo attacco ransomware.

Passaggio 4: Rendi gli attacchi più costosi. Le snapshot SafeMode di Pure garantiscono la resilienza, con backup immutabili che impediscono a hacker o utenti malintenzionati interni di eliminarli, anche utilizzando credenziali di amministratore compromesse. Inoltre, le snapshot SafeMode garantiscono la protezione dei dati in caso di attacco. Grazie alla crittografia incorporata, l'attacco risulta più complicato e costoso. In occasione dell'RSA Conference 2019, Pure Storage e Thales hanno presentato Vormetric Transparent Encryption for Efficient Storage, il primo framework di dati end-to-end per i settori IT e protezione informatica che realizza la data reduction per l'array storage.

Passaggio 5: Rispondi alle minacce ed evolviti. La capacità di reagire, recuperare ed evolversi il più in fretta possibile dopo un attacco è fondamentale. Novità assoluta del settore, la soluzione di data protection moderna all-flash Pure FlashRecover™, progettata in collaborazione con Cohesity®, consente di accelerare il backup offrendo un ripristino rapido su scala.

- Purity ActiveDR™ offre funzionalità di replica dei dati per garantire backup rapidi, mentre FlashBlade offre funzionalità di restore rapido fino a 270 TB/ora.
- Per gli utenti MEDITECH, Pure ha collaborato con BridgeHead Software, Amazon Web Services (AWS) e Healthcare Triangle per offrire backup as-a-service (BaaS), che automatizza la creazione, lo storage e la replica dei backup di MEDITECH su Pure Cloud Block Store™ in AWS.

purestorage.com/IT

+39 02 9475 9422

PURESTORAGE®

©2020 Pure Storage, il logo P di Pure e i marchi indicati nell'elenco dei marchi commerciali di Pure disponibile all'indirizzo https://www.purestorage.com/legal/productenduserinfo.html sono marchi di Pure Storage, Inc. Altri nomi sono marchi commerciali dei rispettivi proprietari. L'uso dei prodotti e programmi Pure Storage è coperto dai Contratti di licenza con l'utente finale, dai diritti di proprietà intellettuale e da altre condizioni, disponibili agli indirizzi https://www.purestorage.com/legal/productenduserinfo.html e https://www.purestorage.com/patents

PS1946-01 11/2020