



Proteggi i tuoi backup dai ransomware

Protezione integrata con CryptoSafeGuard

CryptoSafeGuard è pensato per proteggere le piccole e medie imprese (PMI) dalle conseguenze di un attacco ransomware.

Quando un virus comincia a criptare i tuoi file sorgente, *CryptoSafeGuard* blocca il backup dei file infetti e impedisce che i backup esistenti vengano criptati.

Cosa fa CryptoSafeGuard



Monitora

CryptoSafeGuard controlla che non ci siano tracce di ransomware nei file, nelle cartelle e nelle applicazioni del tuo server sul quale effettui il backup.



Identifica

CryptoSafeGuard identifica comportamenti e attività sospette, ad esempio un ransomware che cerca di accedere ai tuoi backup o criptare i tuoi file.



Protegge

CryptoSafeGuard impedisce ai ransomware l'accesso e la criptazione dei tuoi backup.



Agisce

CryptoSafeGuard ti invia un sms e un'e-mail di alert e blocca tutti i processi di backup.

CryptoSafeGuard: protezione per il backup attiva, semplice e non invasiva

Duplice difesa per il backup

I backup sono l'ultima linea di difesa contro i ransomware. **CryptoSafeGuard** è una tecnologia progettata per tenere i tuoi backup al sicuro e sempre pronti all'uso.

In **modalità Detector** scansiona i dati sorgente per impedire ai file infetti di sostituire i file integri all'interno del backup. In **modalità Protector** invece, *CryptoSafeGuard*, impedisce ai ransomware di modificare i backup esistenti.

CryptoSafeGuard Detector

Quando inizia un processo di backup, *CryptoSafeGuard Detector* opera una scansione per assicurarsi che i dati salvati siano puliti. Utilizza semplici criteri per identificare immediatamente i file sospetti eseguendo poi una serie di analisi sempre più approfondite per confermare la possibile minaccia. Ne risulta una scansione anti-ransomware veloce e non invasiva e, allo stesso tempo, con minori possibilità di identificare falsi positivi.

Questo diagramma mostra come, dopo che un sistema è stato compromesso, il *CryptoSafeGuard Detector* interviene per essere sicuro che l'infezione non si diffonda ai tuoi backup. La fase di ripristino finale (quasi sempre necessaria in caso di infezione ransomware) evidenzia l'importanza di avere un backup "pulito" e protetto.



CryptoSafeGuard Backup Protector

Il *Protector* agisce a monte, monitorando i backup esistenti e impedendo a qualunque processo, diverso da *BackupAssist*, di modificare, cancellare o aggiungere file alle cartelle di backup. Questo livello di protezione è attivo fin dall'esecuzione del primo backup per tenere sempre tutti i tuoi dati al sicuro.

Come ottenere CryptoSafeGuard

CryptoSafeGuard è disponibile per gli utenti che utilizzano BA 10.2 (o una versione più recente). *CryptoSafeGuard* è stato pensato come strumento complementare alle tue soluzioni Firewall e Endpoint Security/Anti Malware.