



Proteggi

i dati del notebook con DigiSAFE DiskCrypt, il disco rigido crittografato.

DigiSAFE DiskCrypt è un dispositivo di memorizzazione di sicurezza costituito da un'unità disco rigido e da un modulo crittografico di tipo hardware che crittografa tutti i dati scritti nel disco rigido garantendo una protezione totale dei dati. DiskCrypt crittografa ogni singolo settore hardware in maniera trasparente, senza influire sulle prestazioni del disco.

DiskCrypt è un componente compatto e facile da installare per le unità disco rigido dei notebook da 2,5 pollici standard. DiskCrypt non richiede l'installazione di driver software o applicazioni ed è indipendente dal sistema operativo. Al termine del processo di installazione, gli utenti possono continuare a utilizzare il notebook come al solito, con la garanzia che i relativi dati siano completamente protetti in caso di furto o perdita del computer.

Crittografia in tempo reale



Autenticazione a due fattori

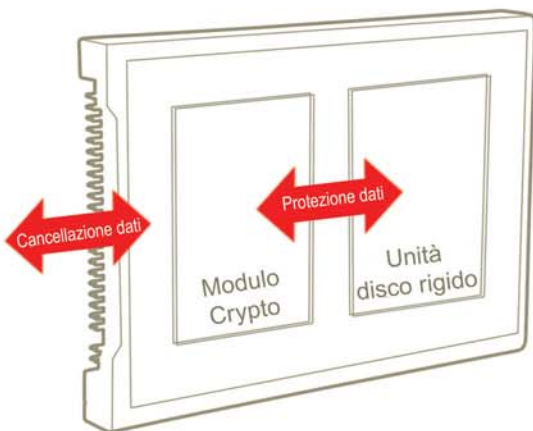


Autenticazione pre-avvio



Crittografia in tempo reale

DigiSAFE DiskCrypt include un'unità disco rigido e un modulo crittografico di tipo hardware che crittografa ogni singolo byte di dati scritti nel disco rigido, in tempo reale e senza influire sulle prestazioni del disco.



FUNZIONALITÀ	VANTAGGI
Crittografia e decrittografia di tipo hardware in tempo reale	Nessuna riduzione delle prestazioni
Soluzione esclusivamente hardware	Trasparenza totale per l'utente, il modulo di crypto è immune da attacchi di virus / trojan e soluzione di software
Crittografia di ogni singolo settore del disco rigido	Totale protezione dei dati
Indipendente dalla piattaforma e dal sistema operativo	Maggiori opzioni operative e flessibilità di distribuzione
Non è necessario installare applicazioni, aggiornamenti o patch	Installazione e manutenzione facili, costo totale di proprietà inferiore
Modulo crittografico hardware antimanomissione	Protezione fisica resistente
Autenticazione pre-avvio	Intenso controllo degli accessi al disco rigido
Supporto dell'autenticazione mediante il token crittografico USB	Autenticazione rigorosa a due fattori
Supporto della migrazione e del backup dei dati	Soluzione di protezione, migrazione, backup e ripristino totale dei dati per notebook

Toolkit di DiskCrypt

Il toolkit di DiskCrypt è costituito da un hard disk enclosure USB esterno e da un'applicazione di clonazione dei dati.

Migrazione:

Consente all'utente di effettuare una migrazione uniforme dall'unità disco rigido originale a DiskCrypt, proteggendo l'ambiente operativo software e i dati dell'utente esistenti.

Backup e ripristino:

Gli utenti possono inoltre effettuare il backup dei dati DiskCrypt in un'altra unità esterna che è possibile archiviare con sicurezza.

Rivenditore autorizzato:

Autenticazione pre-avvio

DiskCrypt autentica l'utente ogni volta che questi accende il notebook o lo ripristina dalla sospensione. I sistemi operativi installati nel notebook verranno eseguiti solo dopo l'autenticazione dell'utente. In DiskCrypt sono disponibili due modalità di autenticazione:

Autenticazione a un fattore:

In questa modalità di autenticazione viene chiesto all'utente di specificare una password nella fase di pre-avvio dopo l'accensione. DiskCrypt autorizza all'accesso solo se si specifica la password corretta.

Autenticazione a due fattori:

In questa modalità di autenticazione viene chiesto all'utente di specificare il token crittografico USB di KeyCrypt USB (in possesso) e la relativa password (nota). DiskCrypt autorizza all'accesso solo dopo che sono stati immessi il token e la password corretti.

	SPECIFICHE
Capacità di memorizzazione	• 20GB, 30GB, 40GB
Velocità di trasferimento dati	• 100 MB/sec Ultra DMA
Interfaccia	• ATA-2/3/4/5/6, SATA 1.0
Velocità di rotazione	• 4.200 rpm
Memoria buffer	• 2MB
Dispositivo fisico	• HDD da 2,5" standard • Conforme a SFF-8200, SFF-8201, SFF-8212 • Dimensioni: 100 mm (L) x 70 mm (P) x 9,5mm (A)
Alimentazione	• 5V 900mA
Sistemi operativi	• Indipendente dai sistemi operativi • Testato con Windows® XP, 2000, ME, 98SE, 98 e Linux
Crittografia	• Motore di crittografia hardware TDES certificato NIST ¹ e CSE ² • Forze chiavi supportate: - DES a 64 bit - 3DES a 128 bit - DES a 192 bit
Autenticazione pre-avvio	• Password • Autenticazione a due fattori con DigiSAFE KeyCrypt
Token crittografico USB DigiSAFE KeyCrypt Token crittografico	• Autenticazione pre-avvio a due fattori
	OPZIONALE
Toolkit DigiSAFE DiskCrypt	• Kit di utilità con - Applicazione di clonazione dischi per la migrazione, il backup e il ripristino dei dati - Hard disk enclosure UB esterno

¹NIST - National Institute of Standards and Technology degli Stati Uniti d'America

²CSE - Communications Security Establishment del governo del Canada

Conformità alle normative

DiskCrypt combina le funzionalità di crittografia dei dati del notebook e di autenticazione pre-avvio per consentire alle organizzazioni di proteggere e controllare meglio gli accessi ai dati aziendali e dei clienti, in conformità a normative quali Sarbanes-Oxley, HIPAA e la Direttiva UE per la protezione dei dati.