

## Modulo Device Encryption

Impedisce l'accesso non autorizzato a computer portatili e computer desktop, con una cifratura completa del disco in modo trasparente e facile da usare. Se un PC con cifratura SafeGuard finisce nelle mani sbagliate, i dati sono illeggibili, anche se il disco rigido viene rimosso.

SafeGuard Device Encryption è un modulo di SafeGuard Enterprise, una soluzione centralizzata per la gestione della protezione di informazioni in ambienti IT misti. (Riferirsi al foglio dati relativo a SafeGuard Enterprise Management Center per informazioni sulla gestione centralizzata)

### Cifratura robusta e trasparente

- Vaste funzionalità di cifratura trasparente
- Cifratura completa del disco (NTFS, FAT, FAT32)
- Algoritmi di cifratura robusti e standardizzati
- Ibernazione protetta e cifrata
- Non è possibile leggere i dati cifrati, nemmeno dopo la rimozione dei dischi fissi dai PC, eccezion fatta per gli amministratori della sicurezza
- Algoritmi di cifratura/decifrazione ad alta velocità

### Autenticazione e autorizzazione protette all'accesso

- Autenticazione utente pre-avvio tramite password, token di cifratura o smartcard, oppure accesso singolo tramite dispositivo biometrico; accesso tramite gruppo di chiavi; azioni di blocco del desktop supportate con token/smartcard<sup>1</sup>
- Accesso unico al sistema operativo
- Regole password definite e attuate centralmente
- Ambiente pre-avvio multiutente con itinerari di controllo
- Aggiunta/rimozione dinamica di utenti registrati dall'ambiente pre-avvio tramite aggiornamenti dei criteri
- Processo di accesso più sicuro, che impedisce attacchi di intrusione diretti a carpire la password
- Schermata di accesso grafica di pre-avvio dal facile utilizzo e personalizzabile
- Gli account di servizio consentono agli amministratori di accedere in modo sicuro a PC di proprietà degli utenti finali

<sup>1</sup> Fare riferimento alla documentazione tecnica di SafeGuard Enterprise per un elenco dettagliato di smartcard, token e dispositivi biometrici (lettori di impronte digitali Lenovo) supportati.

## Vantaggi principali

- » Una sicurezza dati di alto livello, con algoritmi di cifratura comprovati, che ottimizza sicurezza e prestazioni
- » Cifratura di file di scambio e ibernazione per una sicurezza completa
- » Cifratura in background trasparente per l'utente, la quale consente di lavorare senza interruzioni
- » Maggiore produttività per l'utente finale con recupero sicuro della password telefonicamente o tramite l'opzione di autosupporto locale
- » Comodità e velocità per gli utenti finali con accesso singolo al sistema operativo dalla fase di pre-avvio
- » Schermata di accesso grafica di pre-avvio dal facile utilizzo e personalizzabile
- » Maggiore sicurezza con autenticazione tramite impronte digitali biometriche durante il pre-avvio; sono supportati anche token e smartcard
- » Sicurezza dati ampia e completa durante la distribuzione assieme agli altri moduli SafeGuard Enterprise

### Recupero sicuro di password, dati e informazioni di indagine

- Sistema di domanda/risposta via telefono con il servizio clienti per il recupero di password dimenticate
- Opzione di autosupporto locale per recuperare password dimenticate durante il pre-avvio senza la necessità di contattare il servizio clienti o la presenza di una connessione a Internet
- Accesso rapido e sicuro a dischi cifrati su altri sistemi per il recupero o l'accesso di emergenza dei dati, con la riassegnazione automatica delle chiavi abilitata dalla gestione dei gruppi di chiavi di SafeGuard
- Opzione di avvio esterna con Windows PE (ad es. per il recupero di configurazioni di sistemi operativi danneggiati su dischi cifrati)
- Pronto per EnCase (Guidance Software), AccessData e Kroll Ontrack (l'accesso richiede la cooperazione dell'utente o dell'amministratore)
- Supporto per Microsoft Business Desktop Deployment e Computrace
- Integrazione con Lenovo Rescue and Recovery per il ripristino sicuro di sistemi operativi e dati cifrati

### Amministrazione centralizzata

- Criteri di cifratura applicati in maniera centralizzata
- Informazioni relative a utente/computer importate attraverso l'integrazione con i servizi di directory (ad es. Microsoft Active Directory)
- Registri dettagliati effettuano il monitoraggio della conformità
- Dispositivi che non hanno comunicato con il centro gestione a intervalli specifici possono essere bloccati o chiusi in base a criteri mentre sono in linea
- Comunicazione con SafeGuard Management Center mediante protocolli XML/SOAP
- Attività amministrative automatizzate (es. gestione delle patch) abilitate da Secure Wake-On-LAN
- Gestione delle chiavi centralizzata per il recupero e la condivisione dei dati

*Per la gestione centrale è richiesto il modulo SafeGuard Enterprise Management Center. Fare riferimento al foglio dati relativo per maggiori informazioni.*

### Installazione semplice e gestita centralmente

- È possibile distribuire e installare pacchetti di installazione da una postazione centrale e in modo automatico attraverso pacchetti MSI standard.
- La distribuzione in rete è facile—e non richiede il coinvolgimento dell'utente.
- Offre un'opzione di cifratura iniziale rapida, che si occupa solamente delle aree utilizzate di una partizione. Questa opzione velocizza il processo di cifratura/decifratura iniziale.

<sup>2</sup> Per sistemi operativi Mac, riferirsi alla scheda prodotto di SafeGuard Disk Encryption per Mac

### Requisiti di sistema

#### Sistemi operativi<sup>2</sup>

- » Microsoft Windows 7 (a 32 e a 64 bit)
- » Microsoft Windows Vista (a 32 e a 64 bit; SP 1, SP 2)
- » Microsoft Windows XP (a 32 bit; SP 2, SP 3)

#### Certificazioni

- » Utilizza cifratura con certificazione FIPS 140-2
- » Criteri comuni EAL-3+
- » Compatibilità con Aladdin eToken

#### Standard e protocolli

- » Cifratura simmetrica: AES 128/256 bit
- » Cifratura asimmetrica: RSA
- » Funzioni hash: SHA-256, SHA-512
- » Hash delle password: PKCS #5, PKCS #12
- » Smartcard/token: PKCS #15, PKCS #11, Microsoft Cryptographic Service Provider (CSP), PC/SC, Kerberos
- » PKI: certificati PKCS #7, PKCS #12, X.509

#### Versioni in altre lingue

- » Inglese, francese, tedesco, italiano, giapponese e spagnolo
- » Supporto basato su Unicode per altre lingue

*Per informazioni dettagliate, visitare [www.sophos.it](http://www.sophos.it)*