

## Device Encryption-Modul

Das Modul Device Encryption verhindert mittels transparenter und benutzerfreundlicher Festplattenverschlüsselung unbefugte Zugriffe auf Laptops und Desktops. Gelangt ein mit SafeGuard verschlüsselter PC in falsche Hände, sind die Daten selbst bei Ausbau der Festplatte nicht mehr lesbar.

SafeGuard Device Encryption ist ein Modul von SafeGuard Enterprise, der zentralen Lösung zur Verwaltung Ihrer Datensicherheit – auch in heterogenen IT-Umgebungen (Informationen zur zentralen Verwaltung entnehmen Sie bitte dem Datenblatt „SafeGuard Enterprise Management Center“).

### Leistungsstarke, transparente Verschlüsselung

- Breite Auswahl transparenter Verschlüsselungsfunktionen
- Vollständige Festplattenverschlüsselung (NTFS, FAT, FAT32)
- Leistungsstarke Standard-Verschlüsselungsalgorithmen
- Sicherer, verschlüsselter Ruhezustand
- Lesen verschlüsselter Daten unmöglich (mit Ausnahme vom Sicherheitsadministrator), selbst bei Entfernung der Festplatten aus dem PC
- High-Speed-Verschlüsselungs-/Entschlüsselungsalgorithmen

### Sichere Power-On-Authentisierung und -Autorisierung

- Pre-Boot-Authentisierung per Kennwort, kryptographischem Token oder Smartcard bzw. Einmaliges Anmelden unter Verwendung biometrischer Verfahren; Schlüsselring-Zugriff; Unterstützung von Desktop-Sperraktionen über Token/ Smartcards<sup>1</sup>
- Einmaliges Anmelden zum Betriebssystem
- Zentral definierte und durchgesetzte Kennwortregeln
- Pre-Boot-Umgebung für mehrere Benutzer mit Überwachungspfaden
- Dynamisches Hinzufügen/Entfernen registrierter Benutzer aus der Pre-Boot-Umgebung mittels Richtlinien-Updates
- Hochgesicherter Anmeldevorgang, welcher Angriffe über den Kennwortweg praktisch unmöglich macht
- Benutzerfreundlicher und individuell anpassbarer grafischer Pre-Boot-Anmeldebildschirm
- Über Dienstkonten sicherer Administrator-Zugriff auf PCs ohne Verletzung der Endbenutzer-Besitzrechte

## Vorteile

- » Unübertroffene Datensicherheit mit bewährten Verschlüsselungsalgorithmen zur Maximierung der Sicherheit und Performance
- » Verschlüsselung von Auslagerungs- und Ruhezustandsdateien für umfassende Sicherheit
- » Transparente Verschlüsselung, die im Hintergrund und ohne Beeinträchtigung gewohnter Arbeitsabläufe erfolgt
- » Gesteigerte Benutzer-Produktivität dank sicherer Kennwort-Wiederherstellung über Telefon bzw. lokale Selbsthilfe-Option
- » Praktisches und zeitsparendes Einmaliges Anmelden zum Betriebssystem (ab Pre-Boot-Stadium)
- » Benutzerfreundlicher und individuell anpassbarer grafischer Pre-Boot-Anmeldebildschirm
- » Erhöhte Sicherheit mittels biometrischer Fingerabdruck-Authentisierung beim Pre-Boot; Unterstützung von Smartcards und Token
- » Breit gefächelter und umfassender Datenschutz bei Einsatz in Verbindung mit anderen SafeGuard Enterprise-Modulen

<sup>1</sup> Eine detaillierte Liste der unterstützten Smartcards, Token und biometrischen Verfahren (Lenovo-Fingerprint-Modelle) finden Sie im technischen White Paper zu SafeGuard Enterprise.

## Sichere Wiederherstellung von Kennwörtern, Daten und Forensiken

- Herausforderung/Antwort mit dem Helpdesk per Telefon zur Wiederherstellung vergessener Kennwörter
- Lokale Selbsthilfe zur Wiederherstellung vergessener Kennwörter beim Pre-Boot ohne Helpdesk oder Internetverbindung
- Schneller und sicherer Zugriff auf verschlüsselte Festplatten anderer Systeme zum Notfall-Zugriff oder zur Wiederherstellung mittels automatischer Schlüssel-Neuzuweisungen (über SafeGuard Schlüsselring-Verwaltung)
- Externe Boot-Option über Windows PE (z.B. zur Wiederherstellung beschädigter Betriebssystemkonfigurationen auf verschlüsselten Festplatten)
- Vorbereitet für EnCase (Guidance Software), AccessData und Kroll Ontrack (Zugriff erfordert benutzer- oder administratorseitige Kooperation)
- Unterstützung von Microsoft Business Desktop Deployment und Computrace
- Integration in Lenovo Rescue und Recovery zur sicheren Wiederherstellung verschlüsselter Betriebssysteme und Daten

## Zentrale Administration

- Zentrales Enforcement von Verschlüsselungsrichtlinien
- Import von Benutzer- und Computerdaten mittels Integration von Verzeichnisdiensten (z.B. Microsoft Active Directory)
- Detaillierte Protokolle zur Überwachung des Compliance-Status
- Richtliniengemäße Blockierung und Sperrung von Geräten im Online-Zustand, die in bestimmten Intervallen nicht mit dem Management Center kommuniziert haben
- Kommunikation mit SafeGuard Management Center über erweiterte XML/SOAP-Protokolle
- Automatisierung von Administrationsaufgaben (z.B. Patch-Management) dank sicherem „Wake on LAN“
- Zentrale Schlüsselverwaltung zum Austausch und zur Wiederherstellung von Daten

*(Für eine zentrale Administration ist das Modul SafeGuard Enterprise Management Center erforderlich. Mehr Informationen im Datenblatt SafeGuard Enterprise Management Center).*

## Einfache, zentral verwaltete Installation

- Zentrale und unbeaufsichtigte Verteilung und Installation der Installationspakete über MSI-Pakete
- Einfaches Rollout über das Netzwerk – ohne Beteiligung der Benutzer
- Optional schnelle Erstverschlüsselung (verschlüsselt lediglich verwendete Bereiche einer Partition) zur Beschleunigung von Ver-/Entschlüsselung.

<sup>2</sup> Informationen zu Mac-Betriebssystemen finden Sie im Datenblatt „SafeGuard Disk Encryption für Mac“.

## Systemanforderungen

### Betriebssysteme<sup>2</sup>

- » Microsoft Windows 7 (32 und 64 Bit)
- » Microsoft Windows Vista (32 und 64 Bit; SP 1, SP 2)
- » Microsoft Windows XP (32 Bit; SP 2, SP 3)

### Zertifikate

- » FIPS 140-2-zertifizierte Kryptographie
- » Common Criteria EAL-3+
- » Aladdin eToken enabled

### Standards und Protokolle

- » Symmetrische Verschlüsselung: AES 128/256 Bit
- » Asymmetrische Verschlüsselung: RSA
- » Hash-Funktionen: SHA-256, SHA-512
- » Kennwort-Hashing: PKCS#5, PKCS#12
- » Smartcard/Token: PKCS#15, PKCS#11, Microsoft Cryptographic Service Provider (CSP), PC/SC, Kerberos
- » PKI: PKCS#7-, PKCS#12-, X.509-Zertifikate

### Sprachen

- » Deutsch, Englisch, Französisch, Italienisch, Japanisch und Spanisch
- » Unicode-basierte Unterstützung weiterer Sprachen

Vollständige Details unter [www.sophos.de](http://www.sophos.de)