

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 beim Ausbauen 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 Administration entnehmen Sie bitte dem SafeGuard Enterprise Management Center-Datenblatt).

Leistungsstarke, transparente Verschlüsselung

- Breite Auswahl transparenter Verschlüsselungsfunktionen
- Vollständige Festplattenverschlüsselung (NTFS, FAT, FAT32)
- Leistungsstarke Standard-Verschlüsselungsalgorithmen
- Sichere, verschlüsselte Auslagerung von Dateien
- Verschlüsselte Daten können mit Ausnahme vom Sicherheitsadministrator in keinem Fall gelesen werden, selbst bei Entfernung der Festplatten aus dem PC
- High-Speed-Verschlüsselungs-/Entschlüsselungsalgorithmen

Sichere Power-On-Authentisierung und -Autorisierung

- Pre-Boot-Authentisierung per Kennwort, kryptografischem Token oder Smartcard bzw. Single Sign-On unter Verwendung biometrischer Verfahren; Schlüsselring-Zugriff; Unterstützung von Desktop-Sperraktionen über Token/Smartcards*
- Single Sign-On zum Betriebssystem
- Zentral definierte und durchgesetzte Kennwortregeln
- Pre-Boot-Umgebung für mehrere User inklusive Audit-Trails
- Dynamisches Hinzufügen/Entfernen registrierter User aus der Pre-Boot-Umgebung mittels Richtlinien-Updates
- Hochgesicherter Anmeldevorgang, welcher Angriffe über den Kennwortweg praktisch unmöglich macht
- Benutzerspezifischer, grafischer Anmeldebildschirm
- Über Dienstkonten sicherer Administrator-Zugriff auf PCs ohne Verletzung der Enduser-Besitzrechte

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

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 Enduser-Produktivität durch sichere Kennwort-Wiederherstellung über Telefon bzw. lokale Selbsthilfe-Option
- » Beschleunigte Prozesse und erhöhter Enduser-Komfort durch Single Sign-On zum Betriebssystem noch vor Starten des Bootvorgangs
- » Benutzerfreundlicher, graphischer und individuell anpassbarer Pre-Boot-Anmeldebildschirm
- » Erhöhte Sicherheit mittels biometrischer Fingerabdruck-Authentisierung während des Pre-Boot; außerdem Unterstützung von Token und Smartcards
- » Breit gefächelter und umfassender Datenschutz bei Einsatz in Verbindung mit anderen SafeGuard Enterprise-Modulen

Sichere Wiederherstellung von Kennwörtern, Daten und Forensiken

- Challenge/Response 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 user- oder administratorseitige Kooperation)
- Unterstützung von Microsoft Business Desktop Deployment und Computrace
- Integration in Lenovo Rescue and Recovery zur sicheren Wiederherstellung verschlüsselter Betriebssysteme und Daten

Zentrale Administration

- Zentrales Enforcement von Verschlüsselungsrichtlinien
- Import von User- 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 zu SafeGuard Enterprise Management Center.)

Einfache, zentral verwaltete Erstinstallation

- Zentrale und unbeaufsichtigte Verteilung und Installation der Installationspakete über MSI-Pakete
- Einfaches Rollout über das Netzwerk – ohne Beteiligung der Enduser

Systemanforderungen

Betriebssysteme

- » 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)

Zertifizierungen

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

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

² Unterstützung von 64 Bit ab der nächsten Veröffentlichung