

Sensible und wertvolle Daten müssen geschützt werden. Dies gilt vor allem in mobilen Umgebungen, die erhöhte Risiken für unbefugte Zugriffe und ein Mitlesen vertraulicher Informationen bergen. Viele Unternehmen und Organisationen stellen heutzutage ihre Mitarbeiter zur Prozessoptimierung mit mobilen Endpoints aus. Auf diesen Notebooks und Wechselmedien sind organisationsinterne, vertrauliche Informationen wie Forschungsergebnisse, Managementanalysen oder auch Kundendaten gespeichert. In Papierform werden derlei wertvolle Dokumente in Schränken und Tresoren vor Diebstahl und unbefugten Lesern geschützt. Äquivalent bietet SafeGuard PrivateDisk genau diese Schutzfunktion für elektronische Dokumente. SafeGuard PrivateDisk erzeugt ein verschlüsseltes „virtuelles“ Laufwerk auf dem Gerät. Alle sensiblen und wertvollen Daten sind in diesem elektronischen Safe geschützt abgelegt.

SafeGuard PrivateDisk ist in zwei Varianten verfügbar. Die Personal Edition eignet sich hervorragend zum Einsatz in kleinen und mittelständischen Unternehmen, während die Enterprise Edition mit erweiterten Konfigurations- und Verteilungsoptionen die Anforderungen von Organisationen abdeckt.

Viel reisende Manager und Außendienstmitarbeiter profitieren von SafeGuard PrivateDisk Portable: Sie können verschlüsselte Daten auf ihren mobilen Speichermedien überall lesen und gleichzeitig die Sicherheitsstandards ihres Unternehmens einhalten. Zusätzlich bieten die Administrationswerkzeuge und Schnittstellen in der Enterprise Edition von SafeGuard PrivateDisk eine bequeme und kostengünstige Einbindung in die vorhandene IT-Umgebung.

Die Sicherheitslösung erfordert selbst keine zusätzliche Infrastruktur, die Anbindung in eine bestehende PKI (Public Key Infrastructure) ist wahlweise möglich. Um einen stabilen Authentisierungszugriff auf das Dateivolumen zu gewährleisten können für firmenweite Rollouts auch vorhandene Smartcards eingebunden werden.

Vorteile

Erhöhte Sicherheit

- » Elektronischer Safe zum Schutz wertvoller und sensibler Unternehmensdaten
- » Flexibler Datenschutz in Netzwerken, auf lokalen Festplatten, Terminal-Servern und Wechselmedien
- » Einsatz bewährter und vielfach getesteter Sicherheitsalgorithmen
- » Enterprise Edition inklusive Recovery-Zertifikaten, die garantieren, dass auf verschlüsselte Daten im Notfall zugegriffen werden kann

Einfache Installation

- » Zentrale und problemlose Installation sowie Verteilung über Windows Installer bzw. Software-Management-Systeme
- » Keine zusätzlichen Upgrades der bestehenden IT-Infrastruktur erforderlich
- » Skalierbarkeit: Von Einzelgeräten bis hin zum unternehmensweiten Rollout

Benutzerfreundlichkeit

- » Selbsterklärende Funktionen mit hohem Akzeptanzgrad auf Benutzerseite
- » Kein aufwändiges Training der Administratoren und Benutzer notwendig
- » Hohe Flexibilität mit PrivateDisk Portable, das den Zugriff auf verschlüsselte Daten ohne Installation auf fremden Endpoints ermöglicht
- » Durch optional integrierte Schlüsselverwaltung von SafeGuard Enterprise zum Schutz von Daten mehr Transparenz und erhöhte Sicherheit beim Austausch von Daten

Die wichtigsten Funktionen

Sicherheit

- Erstellen eines verschlüsselten virtuellen Laufwerks
- Schnelle und transparente Verschlüsselung durch Simulation eines zusätzlichen Laufwerks
- Schutz für Daten auf Festplatten, Netzwerklaufwerken und portablen Medien wie Disketten, CD-ROMs, DVDs, USB-Sticks und Flash-Speicherkarten
- Benutzerauthentisierung über Kennwort und/oder X.509-Zertifikate
- Optional gemeinsame Schlüsselring-Verwaltung über SafeGuard Enterprise für einfachen und transparenten Austausch verschlüsselter Daten innerhalb von Benutzergruppen des Unternehmens ohne separate Kennwörter
- Unterstützung von Smartcards und USB-Token
- Optionales Löschen des Windows Pagefiles beim Herunterfahren des Computers
- Einsatz des modernsten und führenden Verschlüsselungsalgorithmus AES

Systemadministration

- Schnell implementierbare Lösung mit überzeugendem Preis-Leistungs-Verhältnis ohne zusätzliche Trainings- und Infrastrukturanforderungen
- Windows Installer (MSI)-basierte Installation bzw. Installation unter Einsatz anderer Software-Management-Systeme
- Zentrale Administration sicherheitsrelevanter Einstellungen über Group Policy Objects
- Optionale Integration von Recovery-Zertifikaten, so dass im Notfall auf verschlüsselte Daten Zugriff besteht

Benutzerfreundlichkeit

- Hohe Akzeptanz bei den Anwendern – zusätzliches Training überflüssig
- Parallele Nutzung mehrerer PrivateDisks gleichzeitig
- Teilen einer PrivateDisk zum Austausch gemeinsam genutzter Daten in Gruppen autorisierter Benutzer möglich
- Schützen und Speichern vertraulicher Daten jeder Art auf Notebooks und Wechselmedien
- Nahtlose Integration in Windows Explorer
- PrivateDisk Portable ermöglicht (Lese-)Zugriff auf verschlüsselte Dateien auch ohne Installation

Zertifizierungen

- » FIPS 140-2 (kryptographische Bibliothek in Evaluierung)
- » Aladdin eToken-zertifiziert
- » Gemalto Secure Digital Companion

Drittanbieter

- » Integration von Microsoft Crypto API: durch Cryptographic Service Provider (CSP) können beliebige RSA-fähige Komponenten von Drittherstellern für die Benutzerauthentisierung eingesetzt werden (z.B. Chipkarten oder USB-Token)

Systemanforderungen

Hardware

- » PC mit Intel Pentium- oder kompatibelem Prozessor

Betriebssystem

- » Microsoft Windows 7 (64 Bit)
- » Microsoft Windows 7
- » Microsoft Windows Vista (64 Bit)
- » Microsoft Windows Vista
- » Microsoft Windows XP

Schnittstellen

- » Crypto API/Microsoft Cryptographic Service Provider (CSP)
- » Scripting API zum Einbinden in automatische Administrationsvorgänge
- » LDAP (nur Enterprise Edition)

Standards/Protokolle

- » Authentisierung: Benutzerauthentisierung über X.509-Zertifikate
- » Verschlüsselung: AES (Rijndael) – 128 und 256 Bit-Schlüssellänge
- » Hash: SHA-1

Sprachen

- » Deutsch, Englisch, Französisch, Niederländisch, Spanisch, Portugiesisch (Portugal und Brasilien), Italienisch, Dänisch, Schwedisch, Finnisch, Norwegisch, Japanisch, Chinesisch, Koreanisch