

Der flexibelste Weg zum Schutz von vertraulichen Daten auf mobilen Datenträgern

USB Sticks, Speicherkarten oder optische Medien wie CD und DVD sind aus dem täglichen IT-Arbeitsalltag nicht mehr wegzudenken. Auf allen diesen Wechselmedien lässt sich ein Datenvolumen von mehreren Gigabyte leicht in der Hosentasche oder am Schlüsselbund transportieren.

Leider gehen diese kleinen, mobilen Speichermedien aber auch schnell verloren. Unternehmen und Einzelpersonen stehen gleichermaßen vor der Herausforderung, die auf solchen Medien gespeicherten Daten effizient gegen unbefugten Zugriff zu schützen und den schnellen Export von vertraulichen Daten vom PC oder aus dem Netzwerk auf ungeschützte Wechselmedien zu verhindern. Die daraus resultierenden Anforderungen an den Wechselmedienschutz sind vielfältig: Ein gute Lösung muss in der Lage sein, alle Arten von Datenträgern gleichermaßen abzudecken. Unabhängig davon, ob es sich um Floppy, Memory Sticks, SD/CF Karten oder optische Medien handelt oder das Speichermedium unterschiedlichen Laufwerksbuchstaben zugeordnet wird. Dem zuständigen Administrator muss eine zentrale Definition der Benutzerrechte im Umgang mit Wechselmedien sowie Datenimport und -export ermöglicht werden. Für Benutzer muss eine solche Lösung transparent sein, damit dieser seine übliche Arbeitsweise mit Wechselmedien nicht umstellen muss. SafeGuard RemovableMedia erfüllt diese Anforderungen.

Die Lösung ermöglicht sogar noch mehr: Abhängig von der internen Sicherheitsrichtlinie können mit SafeGuard RemovableMedia geschützte Datenträger auch auf Rechnern verwendet werden, auf denen die Lösung nicht installiert ist. Mitarbeiter, die zu Hause am privaten Rechner arbeiten oder Geschäftspartner können passwortgeschützt auf verschlüsselte Dateien zugreifen. Möglich ist auch die bewusste Mischung von Daten im Klartext und verschlüsselten Dateien, um öffentliche Informationen schnell per Wechselmedium weiterzugeben, ohne die auf dem Datenträger gespeicherten vertraulichen Daten zu kompromittieren.

SafeGuard RemovableMedia leistet diese Fülle an Flexibilität und ist deshalb einzigartig im Bereich des Wechselmedienschutzes. Die einfache, intuitive Konfiguration sowie die transparente Arbeitsweise realisieren optimale Sicherheit bei gleichzeitig hoher Produktivität.

Die Vorteile

Verbesserte Sicherheit

- » Transparente Datenverschlüsselung
- » Unterstützt alle Arten von Wechselmedien
- » Gemischte Verwendung von verschlüsselten und unverschlüsselten Dateien auf ein und demselben Datenträger möglich
- » Zentral durchsetzbare Richtlinien zum Gebrauch von Wechselmedien mit einstellbaren Freiheitsgraden für die Benutzer
- » Verwendung bewährter und geprüfter Sicherheitsalgorithmen, Nahtlose Integration in das Betriebssystem – keine zusätzliche Anmeldung nötig
- » Lokale Datenverschlüsselung in vordefiniertem Ordner

Einfach verteilbar

- » Schnelle und einfache Installation sowie Verteilung über Windows Installer bzw. Software Management Systeme
- » Einfache und flexible Administration mittels Microsoft Management Console
- » Skalierbar von der Einzelplatzlösung bis hin zu einem unternehmensweiten Rollout
- » Integration in kundenspezifische Anwendungen über das Scripting API

Einfach handhabbar

- » Transparente Ver- bzw. Entschlüsselung aller Daten im Hintergrund
- » Intelligente Auswahl der Sicherheitsrichtlinien abhängig vom Datenträgertyp
- » Hohe Benutzerakzeptanz durch einfache und selbsterklärende Bedienung
- » Bearbeitung der verschlüsselten Daten auch ohne Installation auf fremden Endgeräten möglich
- » Optische Medienverschlüsselung integriert in Windows Brennprogramm

Sicherheit

- Schnelle transparente Verschlüsselung auf Wechselmedien sowie in vordefiniertem Ordner auf lokaler Festplatte
- Einsatz des modernsten und sichersten Verschlüsselungsalgorithmus AES mit 256 Bit Schlüssellänge
- Sichere Ableitung der Schlüssel aus den Passwörtern durch Verwendung des standardisierten PKCS#5 Verfahrens
- Schutz gegen das unbefugte Exportieren unverschlüsselter Daten auf Wechseldatenträgern aus dem Unternehmen
- Schutz gegen das unbefugte Importieren unverschlüsselter Daten auf Wechseldatenträgern in das Unternehmen
- Schlüsselsicherung und -wiederherstellung

System Administration

- Windows Installer (MSI) basierende Installation auch mittels anderer Software-Management Systeme möglich
- Programmierschnittstelle zur Automatisierung von wiederkehrenden Administrationsaufgaben
- Zentrale Administration sicherheitsrelevanter Einstellungen durch Active Directory Group Policy Objects
- Group Policy Einstellungen sind unabhängig vom Laufwerksbuchstaben anwendbar
- Verteilung der Unternehmensschlüssel während Setup
- Zentrale Protokollierung

Benutzerkomfort

- Automatische Verschlüsselung ohne Eingriff des Benutzers möglich
- Hohe Akzeptanz bei den Anwendern ohne Notwendigkeit eines zusätzlichen Trainings
- Die gewohnten Arbeitsabläufe der Benutzer werden nicht gestört
- Nahtlose Integration in das Betriebssystem und daher keine zusätzliche Anmeldung nötig
- Alle Arten von vertraulichen Dateitypen können vom Anwender auf wechselbaren Datenträgern geschützt abgelegt werden
- Die Add-on Applikation RemovableMedia Portable ermöglicht den Zugriff auf verschlüsselte Dateien von Wechseldatenträgern auf Drittrechnern auch ohne Installation
- Overlay-Icon zur Kennzeichnung von verschlüsselten Dateien
- Transparente Datenverschlüsselung in vordefiniertem Ordner auf lokaler Festplatte

SGRM 2.0

Systemanforderungen

Hardware

- » PC mit Intel Pentium-Prozessor oder kompatibelem Prozessor
- » Unterstützte Wechselmedientypen:
 - » Speicherkarten wie z.B. CFC, SDC, MMC, SMC, etc.
 - » USB Speichersticks und Festplatten
 - » Firewire Festplatten
 - » CD/DVD-RW
 - » Disketten, Zip, Jazz
 - » Alle weiteren Geräte, die im Betriebssystem als Wechselmedien erkannt werden

Betriebssystem

- » Microsoft Vista 32-bit
- » Microsoft Windows XP 32-bit
- » Microsoft Windows 2003

Zertifizierungen

- » FIPS 140-2

Dritthersteller

- » SafeGuard RemovableMedia ist kompatibel mit allen typischen Softwareverteilungsmechanismen (MSI Pakete)

Schnittstellen

- » Scripting API, um wiederholende Administrationsaufgaben zu automatisieren

Standards/Protokolle

- » 256 Bit Schlüssellänge
- » PKCS#5

Sprachversionen

- » Englisch, Deutsch, Französisch, Japanisch