

SafeGuard RemovableMedia

Silne i transparentne szyfrowanie nośników danych.

Transparentne, jednolite szyfrowanie poufnych danych na wszystkich przenośnych urządzeniach znacznie obniża ryzyko ich utraty bez wpływu na wydajność systemu.

Wygoda i szerokie wykorzystywanie przenośnych narzędzi przechowujących to jedno z największych ryzyk bezpieczeństwa. Napędy USB, dyski zewnętrzne, karty, płyty CD i DVD wielokrotnego użytku przechowują gigabajty poufnych informacji, które bez większego problemu mogą dostać się w niepowołane ręce.

Kradzież czy przypadkowa utrata danych firmy to poważne konsekwencje prawne i znaczne pogorszenie reputacji na rynku. Aby ochronić się przed takimi sytuacjami Sophos SafeGuard RemovableMedia dostarcza Ci mocną szyfrację w każdej postaci dla pełnego zabezpieczenia urządzeń przenośnych bardzo wielu rodzajów.

Mając takie narzędzie możesz być spokojny, że nikt nieuprawniony nie będzie miał dostępu do firmowych danych.

SafeGuard RemovableMedia jest w pełni zautomatyzowany, transparentny dla użytkownika, przez co nie ma żadnego wpływu na jego pracę i wydajność. Wystarczy przeciągnąć dany plik na odpowiedni nośnik i zostanie on automatycznie zaszyfrowany.

Oferuje on także elastyczność funkcyjną dając Ci wybór czy chcesz przechowywać na danym nośniku tylko zaszyfrowane pliki czy również pliki tekstowe. W przypadku, gdy SafeGuard RemovableMedia nie jest zainstalowany na danym urządzeniu, dostęp do zaszyfrowanych danych można uzyskać za pomocą chronionego hasłem samo – rozpakowującego się pliku.

SafeGuard Removable Media to także unikalna funkcja keyring umożliwiająca bezpieczne współdzielenie danych pomiędzy członkami np. grupy projektowej. Opcje centralnego zarządzania zawierają konfigurację Microsoft Active Directory. Interfejs API (application programming interface) daje wtedy możliwość personalizowania administracji, zarządzanie kluczami oraz automatyzację rutynowych zadań administratorskich. Twoje poufne informacje są w dobrych rękach, chronione przez Sophos.

SafeGuard RemovableMedia – Mocna i transparentna szyfrowanie urządzeń przenośnych.

Kluczowe korzyści

Wzmocnione bezpieczeństwo

- Transparentna szyfrowanie danych
- Wsparcie dla wszystkich rodzajów urządzeń przechowujących
- Centralne wzmocnienie reguł korzystania z urządzeń magazynujących przy pomocy konfigurowalnych poziomów bezpieczeństwa użytkowników
- Silne, sprawdzone algorytmy szyfrowania
- Bezproblemowa integracja z systemem operacyjnym – bez dodatkowego logowania
- Szyfrowanie lokalnych plików do pre – definiowanych folderów

Uprozczone wdrożenie

- Szybka, prosta instalacja i dystrybucja dzięki Windows Installer bądź innemu rozwiązaniu zarządzającemu systemami
- Prosta, elastyczna administracja z Microsoft Management Console
- Skalowalne rozwiązanie – od pojedynczej stacji roboczej do całej firmowej sieci
- Integracja z aplikacjami firm zewnętrznymi dzięki skryptowemu API

Uproszczona praca

- Transparentne szyfrowanie i odszyfrowanie w tle
- Opcjonalna kombinacja przechowywania zaszyfrowanych i niezasyfrowanych plików na tym samym urządzeniu
- Automatyczny wybór reguł bezpieczeństwa w zależności od typu narzędzia przechowującego
- Prosty, intuicyjny interfejs użytkownika
- Bez potrzeby doszkalania
- Przeglądanie zaszyfrowanych plików na urządzeniach zewnętrznych bez potrzeby instalowania oprogramowania
- Funkcja keyrign dla bezpiecznego współdzielenia danych wśród członków jednej grupy
- Szyfrowanie urządzeń optycznych zintegrowane z Windows burning wizard

Kluczowe funkcje

Bezpieczeństwo

Szybkie i transparentne szyfrowanie na wszystkich urządzeniach magazynujących i pre – definiowanych folderach lokalnych twardej dysków

Ochrona danych na systemach plikowych FAT, FAT32 i NTFS

Wykorzystanie najnowszych algorytmów Advanced Encryption Standard (AES) z 256 – bitowymi kluczami

Bezpieczna derywacja klucza oparta na PKCS #5: Password – Based Cryptography Standard

Ochrona przed nieautoryzowanym przechowywaniem niezaszyfrowanych danych na urządzeniach magazynujących

Zabezpieczenie przed nieautoryzowanym importowaniem niezaszyfrowanych danych do firmowej sieci z urządzeń magazynujących

Backup'owanie i przywracanie kluczy

Administracja systemowa

• Instalacja oparta na Windows Installer (MSI) bądź przy wykorzystaniu innego oprogramowania zarządzającego systemami

• Interfejs API do automatyzacji powtarzalnych zadań administracyjnych

• Centralne zarządzanie ustawieniami przy pomocy Active Directory Group Policy Objects

• Wysoce granularne ustawienia Group Policy zależne bądź nie ograniczone względem liter napędów

• Wdrażanie firmowego klucza podczas wstępnej konfiguracji

• Centralny rejestr logów

Uproszczona obsługa

• Opcja automatycznego szyfrowania bez interwencji użytkownika

• Bez potrzeby dodatkowych szkoleń pracowników czy administratorów

• Bezproblemowa integracja z systemem operacyjnym (bez dodatkowego logowania)

• Szyfrowanie i przechowywanie wszystkich typów plików

• Aplikacja RemovableMedia Portable Add-on umożliwia dostęp do zaszyfrowanych plików z urządzenia przechowującego na zewnętrznej stacji roboczej bez instalowania SafeGuard

RemovableMedia

• Pre – konfigurowalny folder plaintext

• Szyfrowanie plików do pre – definiowanych folderów lub lokalnych twardej dysków

• Ikonka overlay dla łatwego przeglądania zaszyfrowanych plików

Komplementarne produkty SafeGuard

SafeGuard Advanced Security Plug and Play Management – centralna kontrola modułu plug – and – play

SafeGuard Application Specific Access Rights – konfiguracja praw użytkowników, aplikacji i danych

SafeGuard Easy – bezpieczne szyfrowanie systemów operacyjnych i wszystkich danych przechowywanych na wewnętrznych dyskach twardej

Wymagania systemowe

Hardware

Stacja robocza z procesorem Intel Pentium lub odpowiednim

•

Wsparcie dla urządzeń:

Karty pamięci w tym CFC, SDC, MMC, SMC

Pendrive'y i twarde dyski USB

Twarde dyski FireWire

CD/DVD – RW

Napędy floppy, Zip, Jaz

Inne urządzenia rozpoznawalne przez system operacyjny jako urządzenie magazynujące

System operacyjny

• Microsoft Windows Vista 32 bity

• Microsoft Windows XP 32 bity

• Microsoft Windows 2003

Certyfikaty

• FIPS 140 – 2

Interoperacyjność

•

Kompatybilny z wszystkimi standardowymi mechanizmami dystrybucji oprogramowania (pakiety MSI)

Interfejsy

•

Skryptujący API dla automatyzacji rutynowych zadań administracyjnych

Standardy/Protokoły

•

Klucze AES 256 – bitowej długości

•

PKCS #5

Wersje językowe

•

Angielska, Niemiecka, Francuska, Japońska

•

Planowane rozszerzenie zakresu językowego