

SecureDoc

DISK ENCRYPTION

Szyfruje cały dysk | Dodatkowo pliki, foldery lub partycje | Umożliwia kontrolę dostępu | Trwale usuwa dane | Centralnie zarządzany w firmie

Informacja jest bardzo cennym zasobem. Kradzieże sprzętu komputerowego, podejmowane nie ze względu na sam sprzęt, lecz z powodu informacji na nim zapisanych to niestety zjawisko coraz częstsze. Dlatego też koniecznością staje się zabezpieczanie poufnych danych przed dostępem osób niepowołanych. Rozwiązaniem oferującym użytkownikowi najwyższy poziom bezpieczeństwa są programy szyfrujące całą powierzchnię dysku.

SecureDoc - pełne bezpieczeństwo danych

Szyfrowanie całej powierzchni dysku

Program szyfrując dysk szyfruje każdy jego sektor, dzięki czemu wszystkie informacje, przechowywane są wyłącznie w formie zaszyfrowanej, łącznie z systemem operacyjnym, plikami tymczasowymi, plikiem wymiany, plikami znajdującymi się w koszu oraz plikami, które zostały z kosza usunięte. W ten sposób program SecureDoc rozwiązuje problem braku odpowiedniego zabezpieczenia kopii tymczasowych lub skasowanych plików, które w przypadku stosowania innych programów szyfrujących pozostają niezabezpieczone. Ponadto program umożliwia dodatkowe szyfrowanie pojedynczych plików, folderów czy całych partycji.

Pre-boot authentication - uwierzytelnienie użytkownika przed startem systemu operacyjnego

SecureDoc Disk Encryption wymaga uwierzytelnienia użytkownika (podania nazwy użytkownika i hasła) jeszcze przed startem systemu operacyjnego. Dodatkowo użytkownik ma możliwość zastosowania tokena USB lub karty chipowej z czytnikiem (uwierzytelnienie dwuczynnikowe). Wtedy do uzyskania dostępu do zaszyfrowanych danych użytkownik potrzebuje czegoś co ma - tokena lub karty - oraz czegoś co wie - czyli hasła. Najbardziej wymagającym użytkownikom producent oferuje metodę uwierzytelnienia, w której zbiór z kluczami szyfrującymi zapisany jest bezpośrednio na tokenie lub karcie chipowej.

SecureDoc współpracuje z wybranymi systemami PKI (Infrastruktura Klucza Publicznego), dzięki czemu korporacje z wdrożonym systemem PKI, mogą wykorzystać certyfikaty do uwierzytelnienia w programie SecureDoc. SecureDoc wspiera następujące systemy PKI: CyberTrust, Computer Associates, Digital Signature Trust, Entrust, Identrus, Microsoft, RSAKeon, Thawte, Verisign.

Szyfrowanie za pomocą algorytmu AES z 256-bitowym kluczem

SecureDoc umożliwia szyfrowanie dysku za pomocą algorytmu AES z kluczem 256-bitowym. AES został wybrany i zatwierdzony przez FIPS (Federal Information Processing Standard) do zabezpieczania danych w instytucjach rządowych w Stanach Zjednoczonych. Cechuje się wysoką wydajnością pracy połączoną z najwyższym poziomem bezpieczeństwa. Dotąd nie odnotowano znanych przypadków złamania tego algorytmu. SecureDoc nadal obsługuje algorytmy DES oraz 3 DES dostępne w poprzednich wersjach programu.

Certyfikat FIPS 140-1 Level 2 oraz Common Criteria - gwarancja bezpieczeństwa danych

Program został certyfikowany przez NIST (National Institute of Standards and Technology) jako spełniający wymagania normy FIPS 140-1 Level 2 (Federal Information Processing Standard) uprawniający program do zabezpieczania poufnych informacji na szczeblu federalnym w USA i Kanadzie. Ponadto SecureDoc posiada certyfikat Common Criteria (standard ISO/IEC 15408), uznany przez informatyków przedsiębiorstw i instytucji rządowych na całym świecie. Rządy i instytucje oceniają na jego podstawie poziom bezpieczeństwa i niezawodność produktów technologicznych.



Szyfrowanie całego dysku to metoda gwarantująca najwyższe bezpieczeństwo danych

Wygoda użytkowania

Szyfrowanie danych w czasie rzeczywistym

Proces szyfrowania oraz deszyfrowania zasobów na dysku odbywa się automatycznie w czasie rzeczywistym, co sprawia, że ochrona jest dla użytkownika niezauważalna. Dane są szyfrowane „w locie” w momencie ich zapisu, a deszyfrowane w momencie odczytu.

Możliwość przechowywania zbioru z kluczami szyfrującymi bezpośrednio na tokenie USB lub karcie chipowej

SecureDoc umożliwia zapisanie zbioru Key File (zbioru z kluczami szyfrującymi) bezpośrednio na tokenie USB lub karcie chipowej, co gwarantuje użytkownikowi jeszcze wyższy poziom bezpieczeństwa danych. Poza tym SecureDoc jako jedno z nielicznych rozwiązań na rynku oferuje użytkownikowi szerokie możliwości wyboru tokenów USB, kart oraz czytników. Program doskonale współpracuje w wybranych rozwiązaniach: Safenet, GemPlus, Axalto, Omnikey, Alladin, Rainbow, RSA oraz wielu innych producentów.

Szyfrowanie przenośnych napędów

Program umożliwia szyfrowanie przenośnych napędów ZIP, Jaz, a także szyfrowanie zewnętrznych dysków podłączanych przez USB.

Trwałe usuwanie danych

SecureDoc oferuje również możliwość trwałego usuwania danych. Usuwając dane z dysku - przenosząc wybrany plik do kosza, a następnie opróżniając kosz - tak naprawdę nie kasujemy plików. Stają się one niewidoczne dla użytkownika, ale nadal znajdują się na dysku i są łatwe do odzyskania. Dlatego też konieczne jest trwałe usuwanie danych z tzw. nadpisaniem polegające to na tym, iż w miejscu usuwanego pliku program zapisuje przypadkowe wartości „zamazując” plik tak skutecznie, że niemożliwe jest jego odzyskanie.

Centralne zarządzanie w firmie

SecureDoc Enterprise Server - system centralnej instalacji i administracji kluczami

Program SecureDoc przystosowany jest również do pracy w środowisku korporacyjnym, umożliwiając bezpieczne szyfrowanie dysków nawet w bardzo rozległych sieciach komputerowych, bez ryzyka utraty kontroli nad zasobami. Program pozwala na centralną konfigurację, zdalną instalację (przy wykorzystaniu narzędzi takich jak Microsoft SMS, ZenWorks czy Tivoli) oraz zdalne szyfrowanie dysków na stacjach roboczych.

Administrator może dowolnie tworzyć grupy użytkowników nadając im różne uprawnienia lub zaimportować informacje z istniejących baz takich jak Active Directory. SecureDoc Enterprise Server umożliwia zarządzanie kluczami szyfrującymi, przypisywanie wybranych kluczy określonym użytkownikom, a także zdalne odzyskiwanie dostępu do zaszyfrowanych danych w przypadku utraty hasła zabezpieczającego.

Kontrola dostępu

Poza szeroką funkcjonalnością w zakresie szyfrowania danych program oferuje możliwość blokowania zapisu/odczytu danych z nośników niezaszyfrowanych/zaszyfrowanych, co skutecznie zabezpiecza dane przed przypadkowym usunięciem lub skopiowaniem.

Dodatkowo, w dowolnym momencie administrator ma możliwość zablokowania dostępu do komputera użytkownikowi z ważnym zbiorem KeyFile, jak również ustawienia daty ważności hasła zabezpieczającego.

System etykietowania kluczy szyfrujących

SecureDoc bazuje na unikalnej technologii tworzenia zbiorów z kluczami szyfrującymi oraz przypisywania zbiorom z kluczami etykiet odnoszących się do tożsamości danego użytkownika (np. Jan Kowalski) lub do jego roli w przedsiębiorstwie (np. Dyrektor Działu Sprzedaży). Zastosowanie tej koncepcji pozwala na wygodne współdzielenie zaszyfrowanych zasobów i stworzenie przejrzystej struktury, w której pracownicy pełniący w firmie określone funkcje, mają dostęp do ściśle określonych informacji.

Wymagania sprzętowe

SecureDoc Disk Encryption:

Windows 2000, XP, 2003, procesor Pentium 100MHz lub szybszy, minimum 64MB RAM, 40MB wolnego miejsca na dysku twardym.

SecureDoc Enterprise Server:

Windows 2000, XP, 2003, współpraca z bazami MS SQL, procesor Pentium 166MHz lub szybszy, minimum 64MB RAM, 40MB na dysku twardym.

www.securedoc.pl