ULOTKA PRODUKTOWA

SecureDoc Enterprise

Endpoint Encryption | Device Control

Pełne systemowe szyfrowanie dysków i plików zawsze będzie pierwszą linią obrony.

Administrator rozwiązań,
Sektor przemysłowy
- Gartner Peer Insights (2017)

Zabezpiecza

- Stacje robocze komputery stacjonarne, laptopy, tablety oraz VDI
- Urządzenia przeno ś ne pamięci USB, CD/DVD, karty SD i dyski przenośne.

Chroni przed

- Utratą lub kradzieżą danych
- Niewłaściwą utylizacją dysku
- Nieautoryzowanym dostępem
- Niepowodzeniem audytu przedsiębiorstwa

Same hasła nie są wystarczającą ochroną Twoich danych i urządzeń pełne szyfrowanie dysków jest pierwszą linią obrony. Chroni przed utratą poufnych danych, zapobiega kosztownym wyciekom informacji, a także pomaga osiągnąć kluczowe cele zgodności z politykami bezpieczeństwa.

Mimo to, rozprzestrzenianie danych i urządzeń w Twojej firmie zwiększa złożoność wdrażania pełnego szyfrowania dysków i dodatkowo jest komplikowane przez stale zmieniający się sprzęt, aktualizacje systemu operacyjnego oraz powiększanie ilości mobilnych pracowników. Zabezpieczenie danych w przypadku zgubienia lub kradzieży urządzenia nigdy nie było bardziej konieczne.

WinMagic SecureDoc Enterprise oferuje centralną, zunifikowaną konsolę do zarządzania danymi i ochrony urządzeń. Łączy szyfrowanie pełnego dysku i nośników wymiennych ze sterowaniem urządzeniami oraz portami.

Dzięki SecureDoc Enterprise dane będą nadal chronione na praktycznie każdej platformie sprzętowej lub operacyjnej, nawet podczas migracji z fizycznych do wirtualnych środowisk.

Rozwiązanie dla wyzwań polegających na bezpieczeństwie danych.

Maksymalizacja ochrony poprzez szeroki zakres zastosowania

Chroń dane i urządzenia za pomocą elastycznego, wielosystemowego szyfrowania.

- Szyfrowanie dysku zgodne ze standardem FIPS 140-2.
- Zintegrowane szyfrowanie systemu operacyjnego za pomocą BitLocker lub FileVault 2.
- Wsparcie dla technologii Opal SED
- Zapobieganie utracie danych poprzez szyfrowanie nośników przenośnych, urządzeń granularlnych oraz portów.

Zgodność z politykami bezpieczeństwa oraz poprawa ochrony danych

Zarządzanie i monitorowanie szyfrowaniem z poziomu jednej, centralnie wdrożonej konsoli

- Szybsze wdrażanie szyfrowania dzięki kompatybilnym narzędziom.
- Zarządzanie użytkownikami, kluczami i politykami za pomocą integracji z Active Directory.
- Skrócenie czasu generowania raportów zgodności nawet o 60% przy pomocy jednej konsoli dla wszystkich urządzeń.
- Chroń użytkowników mobilnych i urządzenia za pomocą sieciowego uwierzytelniania przed uruchomieniem systemu operacyjnego (ang. pre-boot).

Obniżony koszt posiadania z szybszym czasem gotowości użytkownika i działu IT

Nie wybieraj pomiędzy produktywnością a bezpieczeństwem. Wyodrębnij to, co najlepsze z obu.

- Skróć czas odzyskiwania hasła nawet o 75%, korzystając z różnorodnych metod oferowanych przez SecureDoc.
- Optymalizacja czasu wydajnej pracy użytkownika, dzięki bezpiecznemu logowaniu / autoryzacji sieciowej.
- Możliwość natychmiastowej reakcji, w przypadku utraty urządzenia, za pomocą zdalnego blokowania, resetowania lub użycia polecenia „kill".
- Efektywne zarządzanie z podziałem na role, odzyskiwanie oraz narzędzia do raportowania.

Jak można ochronić swoje dane w dowolnym miejscu?

Jeśli posiadasz już **SecureDoc Enterprise Endpoint Encryption** rozważ możliwość rozbudowania strategii bezpieczeństwa danych w całym przedsiębiorstwie dodatkowo do punktów końcowych. **Dodaj nowe moduły licencyjne do twojego serwera SecureDoc Enterprise, w tym**:

- **SecureDoc File Encryption** ochrona danych przechowywanych w plikach i folderach lokalnych, a także współdzielonych przez sieć.
- **SecureDoc CloudSync** szyfrowanie danych przechowywanych w chmurze dla rozwiązań EFSS (Eterprise File Sync and Share)
- **SecureDoc for Servers** gwarancja ochrony infrastruktury serwerów fizycznych, z kopiami zapasowymi przed atakami offline.
- **SecureDoc CloudVM** ochrona zadań wirtualnych oraz chmury przed szeregiem znanych zagrożeń.

SecureDoc Enterprise Server oferuje elastyczność w zakresie ochrony danych fizycznych, wirtualnych i w chmurze. Połączenie modułów umożliwia realizację strategii obronnej w celu zapewnienia trwałości oraz stabilności szyfrowania danych, niezależnie od tego, gdzie się one znajdują. **Chcesz wiedzieć więcej? Skontaktuj się z nami!**

www.bakotech.pl | +48 12 376 95 08 | winmagic@bakotech.pl | Ul. Drukarska 18/5, 30-348 Kraków

Specyfikacja techniczna

Wspierane systemy

- Windows 7 Ultimate, Enterprise
- Windows 8/8.1 Professional, Enterprise
- Windows 10 Professional, Enterprise, Education

Szyfrowanie

- SecureDoc Drive Encryption
- SecureDoc File Encryption
- Microsoft BitLocker for Windows
- Apple FileVault 2 for macOS
- TCG Opal 1.0/2.0 SEDs

Walidacja

- FIPS 140-2

Serwery

- Windows Server 2008 lub Wyższe (wersje 32 bit/64 bit)

Bazy Danych

- SQL Server 2008, 2008 R2, 2012
- SQL Server Express 2008, 2012

Scentralizowane zarządzanie i zgodność z rozporządzeniami

SecureDoc Enterprise Server (SES) umożliwia egzekwowanie spójnej ochrony, polityk oraz zgodności we wszystkich urządzeniach i danych w mieszanym środowisku IT.

- Ujednolicony klucz oraz zarządzanie politykami, zsynchronizowanymi z Active Directory, za pomocą jednej platformy.
- Uruchomienie w sieci przewodowej lub bezprzewodowej serwisu PBConnex na etapie „pre -boot" dla szybszego przywracania hasła, aktualizacji polityk oraz bezpiecznego dostarczania kluczy.
- Zarządzaj użytkownikami mobilnymi za pomocą sieci. Upewnij się, że najbardziej podatne na utratę urządzenia są odpowiednio chronione.

Zabezpiecz urządzenie, wraz z systemem operacyjnym, danymi i aplikacjami, za pomocą standardu FIPS 140-2.

Szyfrowanie natywne

- Zaopatrzenie w centralne zarządzanie szyfrowaniem BitLocker oraz FileVault 2, zapewniając stałą kompatybilność i zgodność audytu.
- Wzmocnienie natywnego szyfrowania za pomocą „pre-boot" sieci SecureDoc, umożliwiającą uwierzytelnianie AD, logowanie oraz integracje uwierzytelniania wieloczynnikowego.
- Automatyczne wykrywanie i blokowanie użytkowników przed wyłączeniem lub zawieszeniem szyfrowania BitLocker i FileVault 2 z zaawansowanymi funkcjami zabezpieczeń antysabotażowych.

Ochrona i kontrola urządzeń przenośnych

- W łączanie automatycznego, wymuszonego szyfrowania urządzeń przenośnych, w tym dysków przenośnych, pamięci USB, CD/DVD, kart SD.
- Dostęp do zaszyfrowanych danych z dowolnego urządzenia bez konieczności dodatkowej instalacji oprogramowania lub ograniczeń określonych przez system operacyjny.
- Z astosowanie zaufanych urządzeń i kontroli portów, aby zapobiec utracie danych lub zainfekowaniu złośliwym oprogramowaniem w trybie offline.

Szyfrowanie plików i folderów

- Zmodernizuj agenta SecureDoc Enterprise za pomocą automatycznego oraz transparentnego szyfrowania plików, chroniąc dostęp do danych poszczególnych osób, folderów.
- Nie przerywaj przepływu pracy. Szyfrowanie, odszyfrowywanie i dostęp do danych jest zautomatyzowany dla użytkownika końcowego.
- Centralne, automatyczne lub manualne szyfrowanie poszczególnych plików, folderów, z trwałą ochroną nawet w przypadku wspólnego użytkowania.

		SecureDoc Enterprise	SecureDoc Essentials	SecureDoc Standalone
ZARZĄDZANIE KLUCZAMI	Zarządzanie kluczami i politykami	●	●	
	Zaawansowane raportowanie i narzędzie do audytów	●	●	
	Integracja z Active Directory	●	●	
	Zdalne zarządzanie użytkownikami	●	●	
SZYFROWANIE STACJI ROBOCZYCH	Szyfrowanie całego dysku zgodne z FIPS 140-2	●		●
	Wsparcie BitLockera dla systemu Windows	●	●	
	Wsparcie funkcji FileVault2 dla systemu macOS	●		
	Wsparcie dla sprzętowo szyfrowanych dysków (TCG OPAL)	●		●
	Możliwość szyfrowania plików i folderów (opcja dodatkowa)	●		●
KONTROLA DOSTĘPU	Połączenie sieciowe na etapie pre-boot	●	●	
	Automatyczne odblokowanie przez sieć	●	●	
	Wsparcie dla sieci bezprzewodowych	●		
	Szczegółowa kontrola urządzeń i portów	●		●
	Szyfrowanie nośników wymiennych	●	●	●
	Wieloskładnikowe uwierzytelnianie	●		●
	Reset hasła użytkownika	●	●	