

SecureDoc Essentials

Zaawansowane zarządzanie BitLockerem | Ochrona przed naruszeniem integralności



Doskonała integracja z BitLockerem

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

Zabezpiecza

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

Chroni przed

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

W jaki sposób chronisz poufne dane na stacjach roboczych w firmie?

W przypadku laptopów, komputerów stacjonarnych i tabletów korzystających z systemu Windows 10 większość firm odpowie w ten sam sposób - włączam BitLockera. Z pewnością wiesz, że pierwszym krokiem w tak zbudowanej Twojej strategii szyfrowania powinno być jak najlepsze poznanie narzędzia, w które już zainwestowałeś? Ale czy wiesz, jaki jest drugi krok? Spraw by zarządzanie rozwiązaniem szyfrującym było proste i efektywne.

Szyfrowanie wbudowane w system Microsoft Windows 10 (w wersji Education, Enterprise i Professional) oferuje prosty, ale efektywny sposób ochrony Twoich danych. Ale takie szyfrowanie to zaledwie początek. Potrzebujesz dodatkowego rozwiązania, takiego jak SecureDoc, które zagwarantuje uzyskanie tzw. dowodu zgodności, w przypadku kradzieży lub utraty urządzenia (pomoże udowodnić, że dany sprzęt był zaszyfrowany i spełnia wymogi stawiane przez RODO).

WinMagic SecureDoc Essentials oferuje dwie elastyczne opcje zaprojektowane specjalnie do ochrony, zarządzania i monitorowania rozwiązania BitLocker. Wprowadzając do swojej organizacji rozwiązanie SecureDoc Essentials, nie będziesz musiał utrzymywać i zarządzać oprogramowaniem Microsoft BitLocker Administration and Monitoring (MBAM). To pozwoli Ci ograniczyć koszty i da możliwość bardziej zaawansowanego zarządzania.

Sprawdź jak lepiej korzystać z Bitlockera!

Uprość wdrożenie i zarządzanie BitLockerem

Centralnie wdrażaj, zarządzaj i monitoruj urządzenia, szyfrowane za pomocą BitLockera.

- Szybko identyfikuj niezabezpieczone lub niepodpięte do konsoli urządzenia z BitLockerem i wdróż agenta SecureDoc.
- Wykorzystaj pre-boot BitLockera lub bezproblemowo skonfiguruj pre-boot używając SecureDoc.
- Zintegruj rozwiązanie z Active Directory, by błyskawicznie uruchamiać dowolną liczbę kont użytkowników.
- Zarządzaj centralnie, przechowuj i odzyskuj klucze szyfrujące z jednej konsoli.

Zaawansowane narzędzie zapewniające dowody zgodności

Wzmocnij szyfrowanie swoich dysków stosując regułę "zawsze aktywna".

- Uprość sposób gromadzenia dowodów zgodności, tworząc szczegółowe raporty w dowolnym momencie (na żądanie), a także realizuj audyty bezpieczeństwa w czasie rzeczywistym.
- Zapobiegaj naruszeniu integralności, uniemożliwiając użytkownikom dezaktywację szyfrowania BitLockerem.
- Kontroluj również zdalnie urządzenia zabezpieczone BitLockerem, stosując klucze i obowiązujące polityki.
- Korzystaj z pre-boot SecureDoc w celu szybszej i bezpieczniejszej autoryzacji wieloskładnikowej.

Zredukuj czas przestoju i obciążenie działu IT

Zadbaj, by dział IT skupił się na ważnych zadaniach, a nie zawracał sobie głowy rozwiązywaniem prostych problemów.

- Skróć czas odzyskiwania hasła nawet o 75%, korzystając z różnorodnych metod oferowanych przez SecureDoc.
- Korzystaj z prostego webowego interfejsu przydzielając odpowiednie role użytkownikom.
- Zapomnij o PIN-ach - SecureDoc pozwala autoryzować użytkowników Active Directory i logować ich do systemu za pomocą jednego hasła (Single Sign-On).
- Skorzystaj z niezwykłych zalet funkcji PBConnex oraz z opcji automatycznego odblokowania urządzenia w zaufanej sieci.

Specyfikacja techniczna

Wspierane systemy

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

Wsparcie dla szyfrowania

- Microsoft BitLocker for Windows

Walidacja

FIPS 140-2

Kluczowe funkcjonalności

SecureDoc BitLocker Management (SDBM)

Zaletą wbudowanego w system Windows szyfrowania BitLockera jest prosta i skuteczna ochrona danych, aktualizowana tak samo często jak sam system. SecureDoc BitLocker Management pozwala korzystać z tej możliwości, zapewniając równocześnie zgodność z obowiązującymi w firmie politykami bezpieczeństwa, w tym z wymogami stawianymi przez RODO.

- **ZARZĄDZAJ** urządzeniami szyfrowanymi za pomocą BitLockera - zapewniaj skuteczną ochronę i utrzymuj spójne zasady uwierzytelniania i odzyskiwania kluczy. Wszystko to z poziomu intuicyjnego oprogramowania klienckiego.
- **CHROŃ** urządzenia przed możliwością deszyfracji dysku lub zatrzymaniem ochrony przez użytkownika - nawet tymi z uprawnieniami administratora - korzystając z funkcji ochrony przed naruszeniem integralności.
- **ZAPOBIEGAJ** utracie danych, wymuszając szyfrowanie nośników wymiennych.
- **ZBIERAJ** raporty związane z ochroną i statusem polityk z jednego serwera (SecureDoc Enterprise Server).

SecureDoc On Top of BitLocker (SDOT)

Z SecureDoc prócz podstawowego zarządzania, zyskujesz możliwość elastycznego szyfrowania zintegrowanego z BitLockerem, zarządzanego przez agenta SecureDoc.

- **WZMOCNIJ** ochronę urządzeń przed oprogramowaniem typu passware oraz wymuszonymi atakami typu brute force za pomocą agenta SecureDoc uruchamianego przed startem systemu.
- **KONTROLUJ** poziom dostępu do danych dla każdego użytkownika, wykorzystując możliwość autoryzacji przed uruchomieniem systemu dzięki integracji SecureDoc z Active Directory. Zyskasz też możliwość tworzenia polityki dla poszczególnych użytkowników i grup użytkowników.
- **ZWIĘKSZ** wydajność pracowników, dzięki szybszemu uwierzytelnianiu (Single Sign-On) i automatycznemu odblokowywaniu urządzenia po podłączeniu do sieci zaufanej (PB Connex).
- **ZREDUKUJ** obciążenie działu IT, wykorzystując opcję autoryzacji zaraz po włączeniu komputera (pre-boot) oraz korzystając z możliwości łatwego procesu resetowania hasła, zmiany użytkownika czy zarządzania poprawkami.

	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)	●		●
Szyfrowanie plików i folderów	●		●
Kontrola dostępu			
Połączenie sieciowe na etapie pre-boot	●	●	
Automatyczne odblokowanie przez sieć	●	●	
Wsparcie dla sieci bezprzewodowych	●		
Szczegółowa kontrola urządzeń i portów	●		●
Szyfrowanie nośników wymiennych	●	●	●
Wielokładnikowe uwierzytelnianie	●		●
Reset hasła użytkownika	●	●	

Szukasz bardziej rozbudowanego narzędzia od BitLockera?

SecureDoc Essential świetnie sprawdza się w przypadku ochrony stacji roboczych zabezpieczonych BitLockerem, ale co z innymi urządzeniami i resztą infrastruktury? Rozważ WinMagic SecureDoc Enterprise, który oferuje te same funkcje co SecureDoc Essential, a dodatkowo kompleksowo wspiera szyfrowanie w systemach Windows, macOS, Linux, jak również w sprzętowo szyfrowanych dyskach (TCG OPAL). Co więcej, SecureDoc Enterprise jest zaprojektowany dla większych sieci firmowych, gdzie wymagania zgodności i bezpieczeństwa są bardziej złożone (np. wymagane jest szyfrowanie na poziomie plików, szczegółowa kontrola urządzeń i portów, bezprzewodowa możliwość autoryzacji pre-boot i wielokładnikowe uwierzytelnianie za pomocą inteligentnych kart, tokenów lub danych biometrycznych).

Chcesz wiedzieć więcej? Skontaktuj się z nami!

Dystrybucja w Polsce
DAGMA Biuro Bezpieczeństwa IT
ul. Bażantów 4/2 | 40-668 Katowice

DAGMA
bezpieczeństwo it